MESTRADO EM DIREITO E SEGURANÇA

INTEROPERABILIDADE: CONTRIBUTOS PARA A EFICÁCIA DO PRODUTO DA ACÇÃO DOS ÓRGÃOS DE INTELIGÊNCIA E DE SEGURANÇA DO ESTADO

Dissertação de fim de curso apresentada à
Faculdade de Direito da Universidade Nova de Lisboa,
como requisito parcial para a obtenção
do grau de Mestre em Direito e Segurança.

Autor: AUGUSTO EDUARDO CAPACO

Orientador: Prof. Doutor Francisco Proença Garcia

LISBOA, 2017

Universidade Nova de Lisboa

Faculdade de Direito

INTEROPERABILIDADE: CONTRIBUTOS PARA A EFICÁCIA DO PRODUTO DA ACÇÃO DOS ÓRGÃOS DE INTELIGÊNCIA E DE SEGURANÇA DO ESTADO

Autor: Augusto Eduardo Capaco

Orientador: Prof. Doutor Francisco Proença Garcia

Lisboa, 2017

AGRADECIMENTOS

Os meus sinceros agradecimentos e efusiva saudação dedico, especialmente:

- Aos meus pais, por me terem dado à vida, proporcionando-me assim esse momento inesquecível.
- À Professora Doutora Rosa Maria de Nascimento, esposa e companheira de todos os momentos, mesmo pelas vicissitudes que a vida nos impôs nesta incessante busca do saber, numa altura em que se encontrava na República de Cuba engajada na sua tese de doutoramento, teve sempre a amabilidade de saber e apoiar cada passo da elaboração deste trabalho.
- Às minhas filhas, pelas palavras de incentivo, sobretudo nas suas afáveis perguntas em momentos inesperados "… *quantas páginas o papá já escreveu? Falta muito papá?...*" e pelos sacrifícios consentidos.
- Ao Professor Doutor Francisco Proença Garcia, meu orientador nesta dissertação, pela demonstração de confiança no trabalho por ter aceite este desafio com elevado profissionalismo, aliado a um superior rigor acadêmico que realça a forma epistemológica transmitida ao longo do trabalho.
- Ao Professor Doutor Jorge Bacelar Gouveia, Coordenador do Mestrado de que resultou esta investigação, pelo apoio, incentivo e desafios investigativos colocados.
- Ao Engenheiro Lino Santos, pelo seu enriquecedor contributo, que logo de início aclarou-nos de forma assertiva sobre os conceitos relacionados com a *interoperabilidade*.
- À Direcção do Serviço de Inteligência e Segurança (SINSE), que através do Instituto de Informações e Segurança (InIS) proporcionou-nos a oportunidade de participação deste Mestrado.
- Aos meus chefes e colegas de Serviço, pela compreensão e liberação para frequentar as aulas e a pesquisa da bibliografia da presente dissertação, às vezes em horário de trabalho.
- Ao Director do Gabinete Jurídico do Governo Provincial do Bié e seus colaboradores, pela disponibilidade que tiveram em ceder-me os diplomas legais solicitados para a composição do segundo capítulo.
- Aos meus parentes e amigos, dos quais não me atrevo a nominar.

Muito obrigado a todos!

ÍNDICE

ÍNDICE DE FIGURAS

LISTA DE ABREVIATURAS

A

AC – Acção Coberta

ADM – Armas de Destruição Massiva

C

CIA – Central de Inteligência Americana

COMMINT *Communication Intelligence* – Informações de Comunicações

CSN – Conselho de Segurança Nacional

CI - *Counterintelligence*

CI – Contra-inteligência

CRA – Constituição da República de Angola

D

DEFA – Direcção de Emigração e Fronteira de Angola

DIA – *Defense Intelligence Agency*

DIE – Direcção de Inteligência Externa

DISA – Direcção de Informação e Segurança de Angola

DNI – *Director of National Intelligence*

DoD – *Department of Defense*

DoS – *Department of State*

E

EUA – Estados Unidos da América

G

GEN – Grande Estratégia Nacional

H

H – Hipótese

HUMINT *Human Intelligence* – Informações Humanas

I

IMINT *Imagery Intelligence* – Informações de Imagem

IC – *Intelligence Community*

M

MININT – Ministério do Interior

MINSE – Ministério da Segurança do Estado

MPLA – Movimento Popular de Libertação de Angola

N

NIT – *National Intelligence Topics*

NSC – *National Security Council*

O

OISE – Órgãos de Inteligência e de Segurança do Estado

ONG – Organização Não-Governamental

P

PfP – *Partners for Peace*

PHOTOINT *Photo Intelligence* – Informações de fotografia

Q

QC Questão Central

QD Questões Derivadas

R

RI – Relações Internacionais

S

SIE – Serviço de Inteligência Externa

SIM – Serviço de Inteligência Militar

SISM – Serviço de Inteligência e de Segurança Militar

SIN – Sistema de Informações Nacional

SINFO – Serviço de Informações

SINSE – Serviço de Inteligência e de Segurança do Estado

SME – Serviços de Migração e Estrangeiro

U

URSS – União das Repúblicas Socialistas Soviéticas

US – United States

USA – United States of America

RESUMO

As informações sempre desempenharam um papel de relevo na arte de governar ao longo de toda a História. Desde os tempos mais remotos, os decisores, quando envoltos em ambientes agónicos, procuraram conhecer o meio que os rodeia, de forma a mitigar a incerteza imposta e, com isso, aplicar os meios que possuem com a máxima sobriedade, de modo a atingir objectivos concretos ou salvaguardar os seus interesses.

É assim que, hoje, apenas organizações com características próprias são capazes de produzir informações que permitem propor conhecimento relevante para se formular e implementar políticas direccionadas aos interesses de segurança nacional, lidando com as ameaças e salvaguardando os interesses nacionais. Elas devem ter uma estrutura identificada com a da ameaça principal: menos hierarquizada, em rede, extremamente flexível, com uma eficaz e eficiente coordenação do esforço de pesquisa, alterando o seu paradigma para ser mais cooperativo, multinacional e multidisciplinar.

O objectivo da presente dissertação de mestrado é o de demonstrar a importância e o contributo da interoperabilidade na eficácia do produto da acção dos Órgãos de Inteligência e de Segurança de Estado.

Para tal, procuramos encontrar a compreensão do conceito de inteligência, bem como o entendimento dos sistemas de inteligência e de segurança de Estado. Através de uma análise holística à interoperabilidade na inteligência, cujo enfoque é a sua função na acção dos OISE, perceber que permite a partilha de informações e o reforço da segurança cooperativa no processo de pesquisa, análise e produção de informação.

Palavras-Chave: Eficácia; Informações; Inteligência; Interligação; Interoperabilidade; Segurança.

ABSTRACT

The information has always played an important role in the art of governing all along the History. Since the ancient times decision-makers, when wrapped up in agonizing environments, try to acquire knowledge about the mean surrounding them so they can mitigate the imposed uncertainty and, with that, apply the possible measures with the maximum sobriety, in order to achieve objectives or to safeguard interests.

Today, just organizations with own characteristics are able to produce intelligence that allow to propose important knowledge to formulate and implement politics directed to the national safety interests, working with the threats and safeguarding the national interests. They should have an organization identified with the one of the main threats: Less hierarchized, netlike, extremely flexible, with an effective and efficient coordination of the research effort, changing its paradigm to be more cooperative, multinational and multidisciplinary.

The main objective of the present master´s thesis is to demonstrate the importance and the contribution of systems interoperability in product effectiveness in performance of the Intelligence Organs and State Security.

For such, we try to find a comprehension of intelligence concept, as well as the intelligence systems understanding and of State Security. Through a holistic analysis to interoperability in Intelligence, whose focus is its function in OISE's enactments, we can understand that it allows the intelligence share and the reinforcement of the cooperative security in the research, analysis and production intelligence process.

Keywords: Efficacy; Information; Intelligence; Interconnection; Interoperability; Safety.

INTRODUÇÃO

Impulsionados pela importância capital que deve ter um serviço de inteligência, eis que nos sentimos convidados a proceder a uma investigação cientifica neste domínio, com maior preponderência a uma ferramenta muito hodierna e ainda pouco empregue pelos órgãos de inteligência (a Interoperabilidade). Entendomo-la trazer nesta temática, como contributo para a eficácia do produto da acção dos órgãos de inteligência do Estado.

Se para Maquiavel, o Príncipe necessitava de estar sempre informado, devendo pensar nas desordens futuras e não apenas nas presentes, e por isso, devia servir-se de toda a habilidade para as evitar, pois, prevendo-as à distância, com mais facilidade as poderia remediar (Maquiavel, 2007, p. 49-50), para nós, comungamos com Weiner ao afirmar que "sem um serviço de informações forte, inteligente, dinâmico e activo, os decisores podem ficar limitados na sua liberdade de acção" (Weiner, 2008, p. 15), pois, de modo convergente acrescenta Shulsky que "as informações têm a capacidade de propor conhecimento relevante para se formular e implementar políticas direccionadas aos interesses de segurança nacional, lidando com as ameaças e salvaguardando os interesses nacionais" (Shulsky & Schmitt, 2002, pp. 1-3).

A temática da *intelligence*[1] não é nova para nós. Não é nova pelo facto de ter sido constantemente debatida durante o nosso percurso no Mestrado em Direito e Segurança, que até certo ponto, dominava o centro das atenções a eficácia do produto dos órgãos de inteligência e de segurança do Estado.

Ora, se a *intelligence* foi sempre um assunto que mereceu a nossa atenção ao longo do curso e não só, a dissertação de mestrado, com esta temática, apresentou-se como a grande oportunidade para uma abordagem holística e profunda acerca do contributo da interoperabilidade nos moldes acima referidos.

Tal como colocada, a temática sobre o contributo da interoperabilidade na eficácia do produto da acção dos órgãos de inteligência e de segurança do Estado é, modestamente, *suisgeneres*, rara nos círculos académicos nacionais. Deste modo, e aproveitando-nos deste facto,

[1] Doravante utilizaremos o vocábulo anglo-saxónico *intelligence* para designar as informações de inteligência, pois, foi nossa vontade inserir este vocábulo de elevado valor científico no campo de estudo das ciências sociais e efectuar uma abordagem em português sem perturbar o seu real significado.

entendemos que uma dissertação de Mestrado que versasse sobre esta temática não só seria actual, mas seria também, objectivamente, pertinente e oportuna; motivos mais do que suficientes para que levássemos avante o impulso investigativo que nos fora dado pelo Professor Jorge Bacelar Gouveia nesta esfera e, concomitantemente, fizessemos das insuficiências de fontes e de outras vicissitudes (das quais o facto de não termos elevado domínio de Direito), substratos motivacionais para que tivéssemos pronto, hoje, este trabalho que aqui temos o ensejo de apresentar.

No contexto da cultura de segurança, a segurança nacional constitui tarefa fundamental do Estado. Assim, pretendemos analisar a base conceitual da *intelligence* e o seu contributo à segurança, verificar a sua influência na tomada de decisão, identificando de que forma a interoperabilidade contribui na eficácia do produto da acção dos órgãos de inteligência e de segurança do Estado.

Dada a amplitude da temática, tornou-se necessário delimitarmos o objecto de estudo eleito – a *intelligence* – em três vectores: o primeiro tem que ver com o aspecto geográfico, designadamente a República de Angola, assente nos princípios de um Estado democrático de direito, que partilha valores, direitos, liberdades e garantias, entre outros, e a necessidade de segurança, que se traduz numa necessidade de *intelligence*; o segundo vector, é decorrente do primeiro, no âmbito da sua actuação, ou seja, a política de segurança do Estado; se os Estados democráticos fundamentam-se na legitimidade conferida pelo eleitorado numa lógica de garantir direitos, liberdades e garantias, é legítimo assumir que o esforço da *intelligence* recaia sobre os actores estatais e não estatais no interior ou no exterior do Estado, com base na definição da sua política de segurança; já o terceiro vector, o temporal, foi delimitado ao período pós-11 de Setembro, quando se objectivaram as alterações ao paradigma de segurança dos Estados.

Para uma abordagem mais apurada, elegemos como objectivo geral o seguinte: demonstrar a importância e o contributo da interoperabilidade na eficácia do produto da acção dos órgãos de inteligência e de segurança de Estado. Nesta conformidade, delineamos e respondemos os seguintes objectivos específicos: desenvolver uma base conceptual sobre a *intelligence*, modelos de organização e suas funções; apresentar o quadro jurídico que fundamenta a acção dos Órgãos de Inteligência e de Segurança de Estado; desenvolver uma base conceitual sobre a interoperabilidade e demonstrar a sua importância e contributo na eficácia do produto da

intelligence.

Por conseguinte, foi de todo pertinente que nesta digressão académica, em obediência a metodologia científica, nos propuséssemos a responder a uma pergunta-chave, com vista a mantermo-nos nos carrizes de uma investigação à altura do grau de exigência que este nível académico requer. Eis, portanto, a questão: *Como compreender a importância da interoperabilidade entre os órgãos de segurança do Estado?*

Posto isso, com a colocação do problema acima, surgiram três questões derivadas, que à guisa de variantes, fundamentaram a procura de respostas objectivas para o principal desafio temático proposto, tais como: a) De que forma os modelos de organização da Inteligência contribuem para a segurança do Estado? b) De que forma o ordenamento jurídico nacional contribui na definição da política de segurança do Estado? c) Qual o papel da interoperabilidade na acção dos Órgãos de Inteligência e de Segurança de Estado?

No mesmo sentido, configuraram como hipóteses do nosso trabalho as seguintes: 1- Os órgãos de inteligência e de segurança de Estado constituem estruturas de *intelligence*, facilitadores do processo de decisão política estratégica, enquanto órgãos do Estado. O seu modelo de organização joga um papel fundamental na satisfação das necessidades de segurança do Estado; 2- A República de Angola é um Estado democrático de direito assente na defesa dos direitos, liberdades e garantias fundamentais. A acção dos órgãos de inteligência e de segurança do Estado tem como base a política de segurança nacional definida na CRA e nas demais leis vigentes; 3- A Interoperabilidade na *intelligence* facilita a partilha de informações entre órgãos e satisfaz as necessidades da inteligência básica, com o objectivo de garantir a segurança do Estado.

Na sequência, optamos, fundamentalmente, pelo método dedutivo e por uma pesquisa de tipo qualitativa que priorizou as fontes secundárias (bibliográficas e documentais), num estudo multidisciplinar, implicando os estudos de *Intelligence,* dos diplomas legais vigentes e da Interoperabilidade na administração pública. A maior parte das referências bibliográficas consultadas é relativamente recente. Não obstante, foi possível encontrar referências do final da II Guerra Mundial, ainda que a incidência maior seja desde a última década do século XX até à actualidade, época em que a profusão de estudos – artigos e livros – é maior. Em nosso entender, esta situação encontra enquadramento no vertiginoso incremento de desafios aos

Estados e o consequente ambiente de incerteza na cena internacional, provocado pela globalização e pelo fim do paradigma bipolar.

Com os Estudos de *Intelligence*, porque ainda não é possível identificar uma teoria de *intelligence*, procederemos à análise holística da *intelligence*. Para isso apoiamo-nos em dois autores de referência: Mark M. Lowenthal: «*Inteligência. De secreto para política*»[2]; e Jennifer E. Sims: «*A teoria de inteligência e política internacional*»[3], dois autores que, de certa forma, se complementam. Para Lowenthal «*… inteligência serve e é subserviente da política e ela funciona melhor – analiticamente e operativamente quando ligada à objectivos políticos claramente entendidos*»[4]. O autor, através da análise das actividades de *intelligence*, procura identificar questões específicas que levam a que as estruturas de *intelligence* «*…Ás vezes funcionam bem: Ás vezes não*»[5] (Lowenthal, 2006, 12). Sims, por sua vez, fundamenta a sua análise através do pressuposto que a *intelligence* permite a vantagem de decisão, ao tornar a decisão melhor ou por tornar a do adversário pior. O sucesso não está em garantir a verdade ou a perfeição da informação, está sim em garantir informação suficientemente melhor que permita obter vantagem sobre o adversário.

Com os diplomas legais, analisamos as disposições jurídicas referentes à actividade dos Órgãos de Inteligência e de Segurança do Estado, fundamentalmente sobre quatro eixos principais, nomeadamente: Institucionalização, definição da política de segurança nacional, funções, e os alicerces salvaguardados na legislação para a implementação da interoperabilidade. Com a Interoperabilidade interpretamos a governação electrónica dos Estados e os seus benefícios face aos utilizadores, isto é, a interoperabilidade no centro das atenções do Estado para facilitar a manutenção da comunicação e serviços entre operadores de comunicações electrónicas. Para proceder à análise da interoperabilidade, apoiamo-nos, então, no Regulamento Geral das Comunicações Electrónica aprovado através do Decreto Presidencial n.º 108/16, de 25 de Maio. Este Decreto define o «*acordo de interligação*» e a «*interoperabilidade*».

Por motivos óbvios, salientamos que o presente trabalho foi estruturado em três capítulos:

[2] *Intelligence*. From Secrets to Policy.
[3] *A Theory of Intelligence and International Politics.*
[4] *«… intelligence serves and is subservient to policy and that it works best – analytically and operationally – when tied to clearly understood policy goals».*
[5] «*…Sometimes works well; sometimes it does not*».

1. No primeiro capítulo fizemos um enquadramento conceitual dos sistemas de inteligência e de segurança de Estado, onde efectuamos, num primeiro momento, uma breve análise do conceito de *intelligence*; num segundo, descrevemos de forma sintética o percurso histórico da transformação dos Órgãos de Inteligência e de Segurança de Estado da República de Angola; e em momentos subsequentes, direccionamos a nossa análise, respectivamente, na *inteligência e no contributo à segurança* e nas *estruturas* de forma a perceber qual a razão da existência das mesmas na estrutura burocrática dos Estados; no *conhecimento*, centrada na produção de conhecimento e, necessariamente, na ligação entre decisores e estruturas; nas *funções*, apreciando os factores do ambiente interno que afectam a qualidade do produto dos OISE, tendo em consideração as funções de *pesquisa* e *análise* de *intelligence*; na cultura de segurança, enquanto conjunto de crenças partilhadas, assunpções e formas de comportamentos, derivados da experiência comum e das narrativas aceites (orais e escritas);
2. No segundo capítulo, digredimos sobre as disposições jurídicas referentes a actividade dos órgãos de inteligência e de segurança do Estado, à luz da legislação em vigor, fundamentalmente sobre quatro eixos principais: institucionalização, definição da política de segurança nacional, funções e os alicerces salvaguardadas na legislação para a implementação da interoperabilidade, concentrando-nos em nove diplomas legais, sendo: CRA de 2010; Lei n.º 10/02, de 16 de Agosto[6]; Lei n.º 11/02, de 16 de Agosto[7]; Lei n.º 12/02, de 16 de Agosto[8]; Lei n.º 22/11, de 17 de Junho[9]; Lei n.º 7/17, de 16 de Fevereiro[10], Decreto Legislativo Presidencial n.º 5/12, de 15 de Outubro[11]; Decretos Presidenciais n.º 201/13, de 02 de Dezembro[12] e n.º 108/16, de 25 de Maio[13];
3. No último capítulo, numa espécie de ponto fulcral, fizemos uma abordagem sobre a interoperabilidade, com destaque ao percurso histórico do desenvolvimento das bases de dados, desde os ficheiros elementares dos anos 50/60 até a dependência das sociedades nas TIC´s, no modo de armazenar, recuperar e processar dados que vêm desde os anos 90 aos nossos dias. Aqui analisamos igualmente a base conceptual do

[6] Lei do Segredo do Estado
[7] Lei do Acesso aos Documentos Administrativos
[8] Lei de Segurança Nacional
[9] Lei da Protecção de Dados Pessoais
[10] Lei de protecção das redes e sistemas informáticos
[11] Aprova a Organização e Funcionamento dos Órgãos Auxiliares do Presidente da República.
[12] Aprova o Estatuto Orgânico da Casa de Segurança do Presidente da República.
[13] Aprova o Regulamento Geral das Comunicações Electrónicas.

sistema de gestão de base de dados, fazendo uma alusão conducente a uma percepção de *abstração de dados* em três níveis: físico, lógico e de visão; bem como a governação electrónica dos Estados e os seus benefícios face aos utilizadores, isto é, a interoperabilidade no centro das atenções dos Estados para facilitar a manutenção da comunicação e serviços entre operadores de comunicações electrónicas; dentre outros afins.

Finalmente, realce-se que ao longo do trabalho, procuramos responder, de forma objectiva, a questão central a que nos propusemos, assim como outras questões derivadas; confrontamo-nos com as hipóteses prévias e deduzimos importantes questões de estudos que, tal como devidamente espelhadas na Conclusão, impõe-se, à partida, como um marco que se consubstacia em compromisso para a necessária prossecução investigativa que vá além do primeiro desafio que é o de corresponder a exigência formal que visa a obtenção do grau de Mestre em Direito e Segurança. Queremos com isso dizer que, doravante, tomaremos este trabalho como ponto de partida para o seu aturado enriquecimento, com vista a cosntituir-se num contributo de objectiva mais-valia e sirva de referência no domínio científico em que ele se insere.

CAPÍTULO I

SISTEMAS DE INTELIGÊNCIA E DE SEGURANÇA DE ESTADO

«A Chamada 'presciência' ou 'previsão' não pode ser deduzida dos espíritos nem dos deuses, nem por analogia com os acontecimentos passados, nem por cálculos. Ela deve ser obtida por homens que conhecem a situação do inimigo»[14].

«E, portanto, somente um soberano iluminado e um general valoroso é que são capazes de empregar as pessoas mais inteligêntes como agentes e estarem certos de alcançarem grandes resultados»[15]

[14] San Tsu, «A Arte de Guerra», 1974, p. 293.
[15] Id., ibid., 23, p. 301.

1.1. O PAPEL DAS INFORMAÇÕES NA HISTÓRIA

Desde os tempos mais remotos os decisores, quando envoltos em ambientes agónicos, procuram conhecer o meio que os rodeia de forma a mitigar a incerteza imposta e, com isso, aplicar os meios que possuem com a máxima sobriedade, de modo a atingir objectivos ou salvaguardar interesses.

Assim, o uso de informação pertinente e oportuna pode significar uma redução significativa da surpresa[16] estratégica. Para isso, emergem das brumas do século XIX os Sistemas de Informações Nacionais que evoluíram de meras estruturas *ad hoc*, criadas para satisfazer as necessidades de príncipes durante o tempo de guerra, para organizações estruturadas de forma permanente (Jackson, 2005, p. 21-26).

As Informações desempenharam um papel de relevo na arte de governar ao longo de toda a História. Para Maquiavel, o Príncipe necessitava de estar sempre informado, devendo pensar nas desordens futuras e não apenas nas presentes, pelo que devia servir-se de toda a habilidade para as evitar, pois, prevendo-as à distância, com mais facilidade as poderia remediar[17].

Porém a literatura acerca da temática começa a ter alguma consistência, apenas, a partir da segunda metade do século XX e uma das primeiras abordagens, tendo em vista a perspectiva de análise de sistemas surge, de acordo com Michael Herman (2004, pp. 1-2), em 1949 pela pena de Sherman Kent. Kent faz uma abordagem holística àquele conceito, identificando três elementos: o produto, fazendo referência a um tipo de conhecimento; a estrutura, abordando o tipo de organização que produz o conhecimento; o processo, as actividades conduzidas pela organização.

Posteriormente, seguindo o racional de Kent, Lowenthal (2006, p. 9) sublinha que a abordagem da análise do conceito de *intelligence* deverá ser efectuada tendo em consideração os mesmos três elementos, acrescentando, relativamente a Kent, alguns dados que permitem uma compreensão mais detalhada da realidade. Nesse sentido, faz sobressair que a *intelligence*: (*i*) enquanto processo - deve ser entendida como os meios pelos quais certos

[16] Pode ser entendida como a situação "*that governments (decision-makers, military planners, foreign policy analysts) can never be 100 per cent certain about the current and future motives and intentions of those able harm them in a military sense",* de acordo com Williams, 2008, p. 134.
[17] Cfr. Nicolau Maquiavel, 2007.

tipos de informação são requeridos e solicitados, coligidos, analisados e disseminados e na forma como certos tipos de acção coberta são concebidos e conduzidos; (*ii*) como produto – o resultado do processo, isto é, o conhecimento e as operações, e; (*iii*) enquanto organização – fazendo referência às unidades que conduzem as várias funções da *intelligence*, ou seja, numa perspectiva de «…entidade social composta de pessoas e de recursos, deliberadamente estruturada e orientada para alcançar um objetivo comum» (Chiavenato, 2004, p. 23).

Esta abordagem holística do conceito de *intelligence* permite-nos, então, identificar os elementos essenciais para a construção de uma matriz de análise da noção do conceito de *intelligence*: a organização, o processo e o conhecimento.

1.2. OS ÓRGÃOS DE INTELIGÊNCIA E DE SEGURANÇA DO ESTADO DA REPÚBLICA DE ANGOLA (BREVE PERCURSO HISTÓRICO)

Os Órgãos de Inteligência e de Segurança do Estado têm a incumbência legal de realizar a produção de informações e análises, bem como a adopção de medidas de inteligência e de segurança do Estado necessárias à preservação do Estado democrático de direito e da paz pública (CRA, artigo 212º, nº1).

Os Órgãos de Inteligência e de Segurança de Estado de Angola, antes de constituirem-se em instituição, foram o garante da estabilidade do Movimento Popular de Libertação de Angola (MPLA), na luta contra o colonialismo português e contra as cisões internas do próprio movimento e contra todos os males a que seus dirigentes são propensos (Gizenga, 2013, p. 20). Como instituição, foi constituída a 29 de Novembro de 1975, 18 dias depois da proclamação da independência da República Popular de Angola, com a designação de Direcção de Informação e Segurança de Angola (DISA), ao abrigo do Decreto-Lei n.º3/75.

Razões políticas e estratégicas obrigaram os Órgãos de Inteligência e de Segurança de Estado de Angola a passarem marcantes metamorfoses[18], tais como de DISA para Segurança de Estado, por força da Lei n.º 7/79 em 1979, integrado no Ministério do Interior; ao abrigo da Lei n.º 5/80, através de um ajustamento estrutural é elevado para Ministério da Segurança do Estado (MINSE), em 1981. No período de 1986 à 1988, o MINSE sofre uma reestruturação perdendo algumas das áreas como a Contra Inteligência Militar (CIM), actual Serviço de Inteligência e de Segurança Militar (SISM); a Direcção de Inteligência Externa (DIE), actual

[18] (Gizenga, 2013, p. 20-33)

Serviço de Inteligência Externa (SIE); e a Direcção de Emigração e Fronteira de Angola (DEFA), actual Serviços de Migração e Estrangeiro (SME), integrado no Ministério do Interior.

Com as transformações políticas operadas no país em 1991, que acabaram com o sistema monopartidário, dando lugar ao sistema multipartidário, o MINSE foi extinto. No período que vai desde 1991 à 1992 foi estudado e aplicado um novo modelo desassociado dos modelos anteriores, adaptável a nova era (democrática). Este modelo veio a designar-se Serviço de Informações (SINFO), fundido num novo Ministério do Interior (Gizenga, 2013, p. 24), pelo que o seu Estatuto Orgânico foi adequado apenas em 2008, ao abrigo do Decreto-Lei n.º 1/08.

Por força do Artigo 211º da Constituição da República de Angola (CRA, 2010), foram instituidos os Órgãos de Inteligência e de Segurança de Estado (OISE), nº 2 «A preservação da segurança do Estado compreende componentes institucionais de órgãos de inteligência e de segurança do Estado».

As transformações nas estruturas dos Órgãos de Inteligência e de Segurança de Estado foram operadas por razões de adaptação aos desafios de cada momento. Nesta perspectiva, há uma necessidade contínua de afeiçoar estes serviços a nova era das tecnologias de informação e comunicação.

1.3. A INTELIGÊNCIA E O CONTRIBUTO À SEGURANÇA DE ESTADO

Interessa aprofundar a análise ao conceito de segurança nacional, e perceber como este é preservado pela inteligência.

O Estado é constituído para desenvolver, de forma contínua, organizada e convergente as actividades específicas (ou funções) necessárias à realização dos fins da colectividade política (Ribeiro, 2010, p. 47). A conservação da sociedade política está associada à noção de segurança nacional[19], fim último ou teológico do Estado, condição essencial à preservação da identidade e à sobrevivência de uma unidade política ou, dito de outra forma, à independência e integridade nacionais. Para preservar a identidade e sobreviver, um Estado não deve

[19] A segurança nacional é delimitada pelos interesses que protege. Por isso, pode ser classificada segundo o campo de actuação. A segurança nacional tem por objectivo os interesses nacionais, abarca numerosos campos de actuação e é afectada pelo maior número de ameaças que podem prejudicar esses interesses (Ribeiro, António Silva. *Teoria Geral da Estratégia,* Almedina-Coimbra, 2010, p. 48*).*

sacrificar os seus legítimos interesses à cobiça de outros actores e, em caso de provocação, deve lutar pela sua preservação. Como tal, necessita de estar preparado para fazer face a ameaças multifacetadas e de origens diversas. É no contexto da conservação da sociedade política, que se centra o objeto da estratégia de defesa militar.

Como refere David[20], o conceito de segurança tem sido objecto de uma profunda renovação conceitual, em resultado da evolução dos níveis clássicos de análise da segurança nacional, regional, internacional e cooperativa, proposto pelos realistas e concentrados na capacidade do Estado em conter, autonomamente, as ameaças, para o nível da segurança comum, global e humana, proposto pelos liberais, onde o Estado surge associado a organizações intergovernamentais e a organizações não governamentais para solucionar colectivamente as ameaças. Ciente deste facto, optou-se pelo nível clássico da segurança nacional, não só porque o sujeito da investigação é o Estado, mas, também, porque o seu objeto é o emprego da força militar nas relações internacionais tendo em vista reduzir a insegurança. E, neste contexto, as funções de segurança continuam a ter o Estado como referência primordial.

A segurança nacional foi definida pelo IDN[21] como «a situação que garante a unidade, a soberania e a independência da Nação[22], a integridade e a segurança das pessoas e dos bens; o bem-estar e a prosperidade da Nação; a unidade do Estado e o desenvolvimento normal das suas tarefas; a liberdade de acção política dos órgãos de soberania e o regular funcionamento das instituições democráticas, no quadro constitucional»[23].

O primeiro aspecto evidenciado por esta definição são os interesses nacionais (bens a proteger) que dão corpo à segurança nacional e, pelos quais, em caso de provocação, o Estado deve lutar pela sua preservação. São interesses de carácter nacional, que suscitam duas

[20] David, Charles-Philippe, *A guerra e a Paz, Abordagem Contemporânea da segurança e da Estratégia,* Lisboa, Instituto Piaget, 2001, pp. 29 e 30.
[21] Instituto de Defesa Nacional
[22] As rivalidades franco-alemãs do século XIX fomentaram o desenvolvimento de duas concepções de Nação, uma cívica e outra cultural. A concepção cívica nasceu da Revolução Francesa, que preconizou o direito dos povos se defenderem a si mesmos. A essência da Nação é materializada pelo desejo de viver em conjunto, partilhando valores comuns. Esta concepção é indissociável da democracia participativa. A Nação é uma realidade política compreensível, porque a França, com os EUA, são países de imigração. Assim, adquire-se a nacionalidade escolhendo o lugar onde se deseja viver (direito de solo). Em contraposição a esta concepção, pode encontrar-se, a partir do fim do século XVIII, uma outra originária da Alemanha, país de emigração. A nacionalidade caracteriza-se pela pertença a um povo, pela herança de uma língua e por uma cultura. Nasce-se membro de uma Nação, ninguém se torna seu cidadão (direito de sangue).
[23] Sacchetti, António Emílio, *Temas de Políticas e Estratégia,* Lisboa, Instituto Superior de Ciências Sociais e Políticas, 1986, pp. 21 e 22.

reflexões. Em primeiro lugar, estravasam ligeiramente a concepção vestifaliana de interesses nacionais ligados à soberania, à sobrevivência, ao território nacional e às instituições do Estado, para abarcar outros interesses mais amplos, que exigem soluções regionais e internacionais para conter os efeitos de actores internacionais ligados ao crime organizado, ao terrorismo, à exploração abusiva de recursos comuns, que não se limitam aos territórios nacionais[24].Em segundo lugar, estes interesses nacionais tanto podem ser afectados por actores contrários, que se encontram no exterior, como no interior das fronteiras nacionais. Como tal, não faz hoje sentido continuar a falar-se em segurança nacional interna e externa.

A determinação do actor contrário é uma condição indispensável para centrar todo o problema de segurança nacional, porque evidencia a causa que o determina. A sua identificação e valorização é imprescindível para, no quadro da elaboração da estratégia de defesa nacional, se definir as hipóteses de guerra e os prazos críticos. Porém, a sua localização geográfica não deve servir de base a uma compartimentação do conceito de segurança nacional segundo as fronteiras do país, porque as ameaças são estruturalmente complexas, dispõem de grande mobilidade e possuem um caracter transnacional e difuso, que não respeita esses limites políticos. Nestas circunstâncias, não é possível descodificar verdadeiramente o que constitui hoje uma ameaça para a segurança interna, que não o seja, também, para a segurança externa, nem distinguir uma ameaça que deva ser combatida por forças policiais, que não possa requerer o contributo das forças militares e vice-versa.

A segurança nacional deixou, assim, de ter componentes externas e internas, e passou a reclamar dos Estados outra resposta, com recurso à estruturas orgânicas militares e policiais em perfeita coordenação, de forma a criarem-se efeitos sinérgicos, impossíveis de atingir com compartimentações não concertadas e estanques do próprio Estado.

A definição proposta pelo IDN mostra que, quanto à amplitude, houve uma seleção prudente e séria dos interesses a proteger. Perante a impossibilidade de salvaguardar bens muito extensos e complexos, foi estabelecido o âmbito dos essenciais, sobre os quais devem incidir os esforços de protecção. Assim, o conceito de segurança nacional adoptado inclui, claramente, os interesses de sobrevivência política. Também podem ser identificados no seu enunciado os interesses relacionados com a estabilidade, em que a Nação garante a sua identidade própria, que é reconhecida.

[24] David, Charles-Philippe, op. Cit., p. 26.

Detectam-se, ainda, alguns interesses de desenvolvimento e de realização. Porém, como notou Couto, o conceito de segurança nacional pode ser entendido de forma mais ampla, como abrangendo todo «um conjunto de interesses, que podem ir desde a garantia de acesso a matérias-primas essenciais, até à protecção de investimentos e de cidadãos nacionais no estrangeiro, desde cinturas de segurança a zona de influência ou neutralizadas, desde o controlo do nível da capacidade militar de adversários potenciais e vizinhos, até à uniformidade dos regimes e sistemas políticos, etc. Assim, a preocupação da segurança pode tornar-se tão ambiciosa, que acabe por se transformar em aspiração de ilimitada expansão. A miragem da segurança absoluta exigiria, no plano individual, que se vencesse a morte e, no plano colectivo, o domínio do mundo»[25].

Na ausência de uma autoridade superior, os Estados, como não confiam inteiramente uns nos outros, mantêm as suas capacidades de defesa contra ameaças, a fim de diminuírem a sua vulnerabilidade e aumentarem a sua segurança. Como notou David, é um comportamento generalizado, que traduz, por um lado, a inquietação de todos os Estados em face das ameaças e da insegurança e, por outro lado, a confiança de todos os Estados nas suas Forças Armadas para conter as ameaças e garantir a segurança. Porém, como elas são largamente nacionais, estimulam e mantêm uma situação em que a procura da segurança pode, a qualquer momento, tomar o caminho militar[26].

Sobre esta problemática, Aron evidencia que alguns Estados, para garantir a sua segurança, consideram necessário «o estabelecimento de uma nova relação de forças, ou a modificação da relação existente, para que os inimigos potenciais não sejam tentados a tomar iniciativas de agressão, devido a inferioridade do rival»[27]. Neste contexto, refere a importância de se estabelecer uma relação entre a segurança e a força, porque quanto maior for a força de um Estado, maior será a sua capacidade para se impor aos outros, logo, menor risco de ser atacado.

Seguindo o raciocínio lógico de Aron, um Estado será tanto mais seguro, quanto mais forte. É certo que a força pode ser definida como os «meios, recursos ou capacidades de toda a natureza de que um actor político pode lançar mão ou tirar partido para alcançar os seus

[25] Couto, Abel, 1988, pp. 70 e 71.
[26] David, Charles-Philippe, op. Cit., p. 58.
[27] Aron, Raymond, *Paz e Guerra entre as Nações,* 2ª ed., Brasília, editora universidade de Brasília, 2002, pp. 140 e 141.

objectivos»[28]. Porém, segundo David, é a força militar que representa "para uma maioria de Estados uma das garantias essenciais da sua sobrevivência"[29]. Mas a um aumento de força militar, nem sempre corresponde uma maior segurança nacional. Com efeito, a excessiva edificação de capacidades militares, associada a injustificados sacrifícios económicos e sociais, podem suscitar preocupações de outros Estados que, em consequência, desencadeiam corridas armamentistas e podem, até, lançar ataques preventivos. É o chamado paradoxo ou dilema da segurança[30].

O fortalecimento das capacidades económicas e psicosociais, conjugado com a despreparação das Forças Armadas, torna um país muito vulnerável à coacção militar. Por isso, é importante saber definir, em cada momento, o ponto de equilíbrio de desenvolvimento da força nacional, tendo presente que, por um lado, a segurança se estrutura sobre uma base de desenvolvimento económico e social, abaixo da qual se degrada a capacidade de se realizar esforços estratégicos e que, por outro lado, o desenvolvimento se estrutura sobre uma base de segurança. Abaixo da qual não se dispõe da capacidade de preservação dos interesses económicos e sociais.

As considerações acerca da relação entre a força e a segurança evidenciam a importância do nível de protecção a alcançar. Isto é, a expressão da necessidade sentida pela Nação de proteger os seus interesses, garantindo a coerência entre o que se deseja, aquilo que é possível e a vontade de agir. Estes três elementos estão interrelacionados de tal forma que se afectam reciprocamente, e a segurança nacional dependerá da resultante das três dimensões.

Assim, a segurança nacional desejável é uma meta a alcançar, que traduz à medida que se deseja neutralizar cada um dos actores contrários. Para esta concepção de segurança desejável, poderá estabelecer-se um nível mínimo, que é o objectivo prioritário a alcançar, e

[28] Couto, Abel, (1988, p. 42).
[29] David, Charles-Philippe, op. cit., pp. 58 e 59, considera que este facto traduz o dilema de defesa, manifestando "pela existência e pela influência muito dominante das forças militares, símbolo musculado da persistência do Estado armado de Vestefália".
[30] O dilema da segurança resulta da situação de anarquia em que o sistema internacional de Estados se encontra. Tentando aumentar a sua segurança, pela adopção de políticas que desenvolvem as respectivas capacidades militares, os Estados, inadvertidamente, levam a que os outros se sintam menos seguros. Como refere David, Chrales-Philippe, op. Cit., p. 60, "no final de contas, a segurança procurada e obtida por uns origina a insegurança dos outros". Em consequência deste comportamento, desenvolve-se um círculo vicioso ou espiral de segurança – insegurança, para o qual não há uma solução permanente e duradoura. A confiança bipolar da Guerra-Fria exacerbou este dilema para níveis muito superiores aos dos sistemas da balança de poderes.

um nível máximo, que é o objectivo ideal. Como na opinião de Martin[31], é impossível colocar este nível máximo nos 100% de segurança nacional, tornando-se necessário admitir um diferencial traduzido pelo risco aceitável, isto é, pela probabilidade e periculosidade de uma perda potencial, admitida em resultado da concretização de uma ameaça. A segurança nacional possível resulta da comparação global dos actores contrários, com as possibilidades e meios próprios para proteger adequadamente os interesses nacionais.

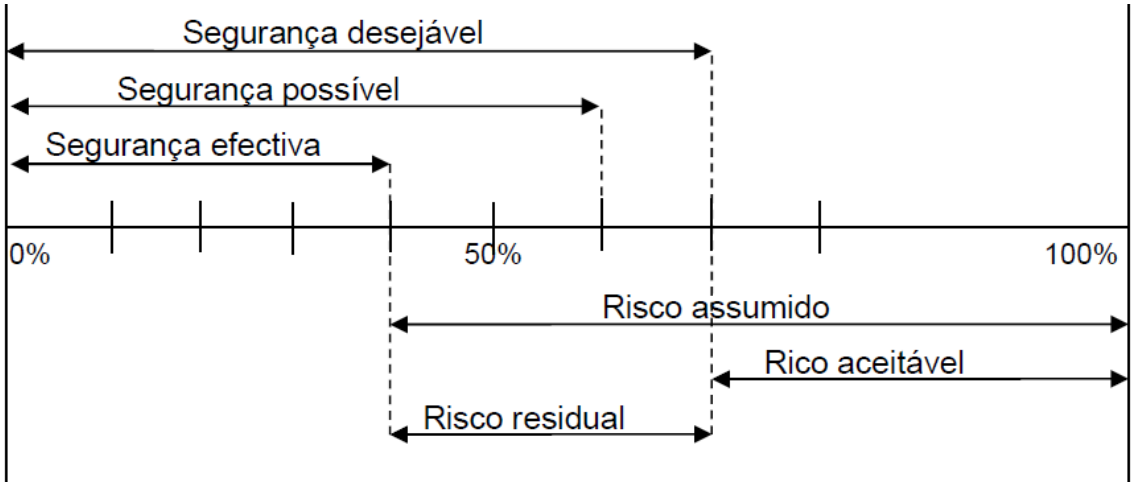


Fig. 1.1 – Níveis de protecção a alcançar[32]

Para cada interesse nacional estabelece-se a segurança efectiva, fruto da prioridade que se atribui à sua protecção. Desta forma, pode ponderar-se a segurança nacional, incrementando a de determinados interesses com uma maior cobertura, em detrimento da de outros, fazendo-a aproximar-se mais ou menos da segurança desejável. A diferença remanescente entre a segurança efectiva e a segurança desejável, traduz um risco residual, isto é, a probabilidade e periculosidade de uma perda potencial, possível em resultado da concretização de uma ameaça. Se este risco for considerado inaceitável, pode ser reduzido actuando sobre a cobertura, quando se dispõe de meios para o efeito, ou diminuindo os interesses a proteger, de forma a proporcionar aos restantes o grau de segurança considerado necessário. Em todo caso, há sempre um risco residual que, acrescido ao risco aceitável, dá origem ao risco assumido.

[31] Martin, Miguel Ángel Ballesteros, «Las estratégias de Seguridad y de defensa», *Fundamentos de la estratégia para el Siglo XXI*, s.d., Centro de estudios de la defensa Nacional, nº 67, dezembro 2003, p. 32.
[32] Martin – Ibid, ibidem.

Isto é, a probabilidade e periculosidade de uma perda potencial, evocada em resultado da concretização de uma ameaça.

Para tal os Estados dispõem de outras estruturas «incumbidas de realizar a produção de informações e análises, bem como a adopção de medidas de inteligência e de segurança do Estado necessárias à preservação do Estado democrático de direito e da paz pública»[33].

No caso da república de Angola, a sua Constituição salvaguarda a preservação da segurança do Estado «tem por objectivo a salvaguarda do Estado democrático de direito contra a criminalidade vilenta ou organizada, bem como outro tipo de ameaças e riscos, no respeito da Constituição e das leis, bem como das convenções internacionais de que Angola seja parte» (CRA, artigo 211º nº1). No nº 2 do mesmo artigo esclarece-se que «a preservação da segurança do Estado compreende componentes institucionais de órgãos de inteligência e de segurança do Estado», ficando claro deste modo que a inteligência joga um grande contributo à segurança.

Ao falar de *intelligence* com alguma facilidade se identificam, no imediato, estereótipos associados ao secretismo e à espionagem, percepção para que, por certo, muito contribuíram as obras de Ian Fleming ou John Le Carré, entre outros. No entanto, de acordo com Keegan (2006, pp. 4-5), ainda que estas traduzam algum fundo de verdade, a realidade é muito mais abrangente, sendo possível identificar, a utilização deste conceito[34] sob dois prismas.

No primeiro, numa noção *latu sensu*, assume-se que a *intelligence* é toda a informação pesquisada, organizada ou analisada de forma a satisfazer as necessidades de qualquer decisor, desde que envolto numa empresa de competitividade.

Nesse sentido, Jennifer E. Sims, uma académica das Relações Internacionais (RI) que desempenhou, cumulativamente, várias funções de relevo na área da *intelligence*[35], no Departamento de Estado (DoS) dos Estados Unidos da América (EUA), apresenta a *intelligence* como sendo «*…a colecta, análise, e disseminação de informação para aqueles*

[33] (CRA, artigo 212º, nº 1)
[34] Ao entendermos conceito como uma apresentação ou representação intelectual e abstracta da essência de um objecto, facilmente percebemos que será necessário isolar e apreender, de um objecto concreto, "determinada nota ou conjunto de notas essenciais que o caracterizam ou definem" (Freitas, 1989, p. 1078).
[35] Das quais se destacam *Deputy Assistant Secretary of State for Intelligence Coordination* (1994-1998) e *Intelligence Advisor to the Under Secretary for Management and Coordinator for Intelligence Resources and Planning at the US Department of State* (1998-2001).

que tomam decisão e ocupados em iniciativa competitiva»[36] (2009, p. 62). A autora entende *competitive enterprise* numa perspectiva abrangente que prevê os negócios, a política, o desporto ou outra, importa, apenas, que os objectivos sejam o cerne da competição. O foco desta académica é o produto, cuja finalidade é a de facilitar as tarefas dos decisores, empenhados em competição, de onde sobressai uma percepção de presente. A noção da Doutora Sims, traduz que o conhecimento[37], desenvolvido ao nível académico, num qualquer ensaio, desde que destinada a decisores envolvidos em actividades de competição é *intelligence*.

As observações de Adda Bozeman, citada por Warner, reforçam a perspectiva de Sims quando aquela autora observa que Estado não é a unidade de trabalho decisiva no estudo da *intelligence «…tomando decisões relevantes…emana crescimento em gente espalhada, frequentemente dissimuladas as frentes dos postos-comando de deliberação, brigadas de terroristas, governos provisionais, ou partido comunista internacional»*[38] (Warner, 2009, pp. 17-18). Warner atribui àqueles actores a categoria de *soberanias*, onde inclui os Estados-nação, em virtude da possibilidade de usarem a violência, procurar o controlo de populações, recursos e território. Segundo aquele autor, são estas as características que diferenciam as *soberanias* dos restantes actores cuja rivalidade é meramente comercial, financeira ou desportiva (Warner, 2009, p. 18). Porém, o que distancia os actores Estatais, das restantes *soberanias*, é a legitimidade inerente ao Estado[39], por um lado, e o cariz subversivo, inerente aos segundos por outro, para quem a necessidade de *intelligence* passa, em grande parte, por

[36] «…the collection, analysis, and dissemination of information for decision makers engaged in a competitive enterprise»

[37] De acordo com Edward Waltz (2003, p. 3) há três níveis de abstracção de conhecimento. Os DADOS – observações individuais, medidas e mensagens primitivas do nível mais baixo (os termos informações em bruto – *raw intelligence* – e evidências são utilizados, de forma frequente, para designar elementos de dados. A INFORMAÇÃO – grupos de dados organizados (o processo de organização pode incluir a classificação, a indexação e a ligação de dados de forma a contextualizar os elementos dos dados para subsequente pesquisa e análise). O CONHECIMENTO – a informação uma vez analisada, compreendida e explicada é conhecimento ou estimativa, o produto das informações (a percepção da informação providencia um grau de compreensão dos relacionamentos estáticos ou dinâmicos dos objectos de dados e da capacidade de modelar a estrutura e comportamentos passados desses objectos), o conhecimento inclui conteúdo estático e processos dinâmicos.

[38] *«…relevant decision making…emanates increase in guys from scattered, often dissimulated command posts of liberation fronts, terrorista brigades, provisional governments, or international communist parties».*

[39] "Classicamente, revelam a existência de soberania três direitos dos Estados: jus tractuum, ou direito de celebrar contratos, o jus legationis ou de receber e enviar representantes diplomáticos e o jus belli ou de fazer a guerra…*"* (Miranda, 2002, p. 189)

uma necessidade de sobrevivência de organizações clandestinas[40] e não por uma necessidade de prosseguir um determinado interesse nacional[41].

Assim, ao nível dos actores estatais, a *intelligence* possui um significado mais restrito. Está, por norma, associada às RI, à política externa, à defesa, à segurança nacional e, consequentemente, ao segredo e às instituições designadas de serviços de *intelligence* (Herman, 2004, p. 1). A *intelligence* apresenta-se como um facilitador das escolhas necessárias para atingir os fins últimos do Estado[42].

Seguindo o racional de Herman, o Professor Heitor Romana refere que numa definição alargada, «estas corresponderão ao conhecimento de elementos estáticos e dinâmicos úteis à escolha, regulação, orientação, monitorização e antecipação de medidas e acções consideradas como estruturantes ou axiais para o planeamento da condução da política dos programas governativos» (2008, p. 98).

De acordo com o mesmo autor, a informação é coligida e tratada ao nível dos gabinetes políticos sendo, após este processo, incorporada no processo da actuação da política corrente. Salientamos a preocupação do autor, em sublinhar a acção governativa, no que concerne à finalidade da *intelligence*, excluindo todo o tipo de conhecimento que gravite fora da esfera do Estado.

Num segundo prisma, *stricto sensu*, a *intelligence* deve ser entendida como a pesquisa de *intelligence* sem o consentimento, a cooperação ou o conhecimento dos «alvos», de forma a alimentar as necessidades do Estado, tendo, por isso, o segredo um papel fulcral.

[40] Em virtude das actividades que desenvolvem, causam atrição à autoridade do Estado, o que leva a que, por questões de sobrevivência procurem a clandestinidade, levando a que operem, necessariamente, em segredo.
[41] O interesse nacional "diz respeito adirectrizes fundamentais que regem a política do Estado relativamente ao seu ambiente externo (…) são um conjunto de diversas e subjectivas preferências que mudam periodicamente em resposta quer ao processo político interno quer do ambiente externo (…) o que parece ressaltar quanto ao interesse nacional é a segurança, ou seja, a sobrevivência do Estado independente na comunidade internacional, a integridade do território, a população intacta, a economia em desenvolvimento e as características culturais próprias*"* (Sousa, 2005, p. 105).
[42] Marcello Caetano *apud* Lara (2004, p. 257) refere que à sociedade política são atribuídos, classicamente, os fins de: segurança – para as pessoas e para os valores que constituem a sociedade política; Justiça – como garante da paz entre as pessoas e os grupos sociais através do respeito mútuo e equidade; bem-estar material e espiritual – as pessoas e grupos sociais são importantes para, de uma forma isolada, satisfazer as necessidades de cultura e economia, cabendo ao poder político, em maior ou menor escala, o provimento da satisfação dessas necessidades.

De acordo com Shulsky muita da informação necessária para a decisão dos governos é acedida por vias informais ou mecanismos não-estruturados – *media*, negociações oficiais, viagens, contactos com académicos, contactos com executivos de negócios e outros – porém, estes, são manifestamente insuficientes se um decisor tiver necessidade de determinado tipo de informação[43] que apenas os mecanismos organizados e estruturados possam facilitar (1995, p. 17). Para além do mais, é inerente a necessidade de «tratamento especial», sendo o segredo uma característica destes mecanismos. Deve, então, entender-se *intelligence* como segredo ou informação secreta (Shulsky, 1995, p. 26). Assim, a *intelligence* foca-se numa determinada tipologia de informação, necessária às escolhas dos decisores, carecendo de ser conduzida por mecanismos organizados e estruturados para o efeito.

Nessa perspectiva, para Heitor Romana, o conceito de *intelligence* é entendido, em sentido restrito, como «um processo de obtenção de conhecimento fundamental à tomada de decisão quanto à salvaguarda dos interesses permanentes ou conjunturais dos Estados, assumindo uma natureza e finalidade ofensiva e defensiva» (2008, p. 98). Nesta noção, o autor, apresenta-nos a *intelligence* numa perspectiva holística, isto é, enquanto processo, produto e organização. Relativamente ao processo, Romana, introduz, explicitamente, a ideia de conhecimento. Para que tal seja possível é necessário um conjunto de actividades que variam desde a manifestação das necessidades, pelo decisor, até à disseminação ao decisor, induzindo uma necessidade de relação biunívoca entre as organizações e decisores.

O referido conhecimento é, então, aquele que garantirá o alerta precoce, bem como a constante monitorização das situações que se tornem fundamentais à tomada de decisão, o autor apresenta-nos a ideia das necessidades de futuro, bem como, de presente. Não sendo, então, todo o conhecimento enquadrado nesta noção, apenas aquele que é fundamental à tomada de decisão relativa ao interesse nacional – permanente ou conjuntural. Deste modo, remete-nos para a organização uma vez que uma das características desta informação e das necessidades decorrentes do processo de decisão é, precisamente, a necessidade de segredo. A este propósito, Lowenthal refere que *«...segredo não faz inteligência excluisiva. Que os outros gostariam de guardar informação impotante a ti, que tu precisas com certeza o tipo de informação e desejas manter o seu necessário segredo»*[44] (2006, p. 4). Pelo que, apenas

[43] Política, militar, económica, social, ambiental, cultural e sanitária, entre outros.
[44] *«…secrecy does make intelligence unique. That others would keep important information from you, that you need certain types of information and wish to keep your needs secret»*

organizações com características próprias permitem atingir este desiderato, são os OISE, de tutela do Estado. Além disso, esta noção permite-nos entender a *intelligence*, quanto à natureza, com uma actuação defensiva e ofensiva, em relação a actores cujos objectivos sejam conflituais ou potencialmente conflituais com os do próprio Estado.

Sistemas de Informações Nacionais transmitem a ideia de como são organizadas, de forma permanente, tratadas e executadas determinadas necessidades de conhecimento secreto, necessário para que os Estados possam perceber e influenciar a incerteza que lhe é colocada pelo meio externo e que escapam ao seu controlo (Warner, 2009, p. 24), de forma a facilitar o processo de tomada de decisão, no quadro da política interna ou externa. Enquanto organizações são órgãos do poder executivo tendo como consumidores os chefes de Estado ou de Governo ou outras autoridades da administração pública, que conduzem as suas actividades[45] em ambientes adversos, como podemos constatar no Decreto Legislativo Presidencial n^{o}5/12, de 15 de Outubro, capítulo VIII, secção I, que estabelece a composição dos órgãos de Inteligência e de Segurança de Estado, como Órgãos e Serviços Específicos Auxiliares do Presidente da República e Titular do Poder Executivo[46].

1.4. MODELOS DE ORGANIZAÇÃO DA INTELIGÊNCIA

Sem um serviço de informações forte, inteligente, dinâmico e activo, os decisores podem ficar limitados na sua liberdade de acção (Weiner, 2008, p. 15). As informações têm a capacidade de propor conhecimento relevante para se formular e implementar políticas direccionadas aos interesses de segurança nacional, lidando com as ameaças e salvaguardando os interesses nacionais (Shulsky & Schmitt, 2002, pp. 1-3).

Segundo Romana (2008, p. 98), as informações podem proporcionar a liberdade de acção, fornecendo conhecimento de elementos estáticos e dinâmicos úteis à escolha, regulação, orientação, monitorização e acções de antecipação de medidas consideradas estruturantes, e axiais para o planeamento da condução política.

Apesar da dispersão verificada no vector conceptual, torna-se importante manter a estrutura de toda uma organização que trabalhe num determinado processo de informações. A

[45] Pesquisa, análise, *counterintelligence* e acção-coberta.
[46] Nos seus artigos 49^{o}, 50^{o} e 51^{o} respectivamente, compõem *"Serviço de Inteligência e de Segurança de Estado, Serviço de Inteligência Externa e serviço de Inteligência e de segurança Militar"*.

creditação da estrutura determina o sucesso da actividade das informações dessa organização (Hannah, O' Brien, & Rathmell, 2005, p. 4)

Ao nível da hierarquização, as informações podem operar com distintas abordagens, por vezes em simultâneo: (i) um processo de recolha e análise; (ii) uma organização que operacionaliza o processo de informações; e, (iii) um produto que é entregue aos decisores (Hannah, O' Brien, & Rathmell, 2005, p. 6).

Neste caso, é necessário diferenciar as informações estratégicas das informações tácticas, que são geralmente mal interpretadas. Enquanto as informações estratégicas efectuam avaliações de cenários com análises prospectivas, as informações tácticas contribuem directamente para o sucesso de investigações específicas (Peterson, 2005, p. 3). As informações estratégicas são então uma espécie de conhecimento, um subconjunto especializado composto por um processo analítico para apoiar a decisão de um Estado (Hannah, O' Brien, & Rathmell, 2005, p. 3).

As informações supramencionadas são como uma organização quando o seu estudo é integrado e relacionado com a legislação nacional em vigor em cada Estado, estabelecendo uma organização funcional que permita desencadear actividades de obtenção de informações (Duvenage, 2010, p. 5).

Vários factores podem contribuir para a alteração das estruturas estabelecidas na comunidade de informações, factores esses que podem ser sistematizados da seguinte forma: (i) as regras e leis adoptadas por um ou mais serviços, como são versados entre a comunidade de informações e outros actores no âmbito da segurança e defesa; (ii) a forma como a análise processa a informação recolhida; (iii) a necessidade de centralizar o comando e controlo dos serviços de informações; e, (iv) a necessidade de assegurar a compreensão exterior à conjuntura da comunidade de informações sobre a actividade da mesma (Hannah, O' Brien, & Rathmell, 2005, p. 6).

As diferentes estruturas podem influenciar significativamente os serviços de informações e respectiva actividade, na recolha de informação e acções encobertas, face à respectiva legislação em vigor (Shulsky & Schmitt, 2002, p. 2).

O interesse do Estado, desde o fim da guerra-fria, é cada vez mais afectado por actores cuja indefinição dos contornos impede a aplicação dos elementos tradicionais de poder. A importância da *intelligence*, enquanto facilitador do interesse nacional é absolutamente primordial. Jorge Silva Carvalho refere que «os serviços de informações constituem, actualmente, a primeira linha da defesa e segurança [do Estado]… » (2006, p. 92) continua fazendo alusão a que «o puro poder militar já não é suficiente para combatê-las [ameaças e desafios] com absoluta eficácia, nem mesmo é possível, à maioria dos Estados, manter um poder militar efectivamente dissuasor … » (2006, p. 93). De facto, a «paz longa» marcada pela estratégia da dissuasão nuclear, alimentada pelo medo de uma «vitória de Pirro», que marcava o equilíbrio do sistema, como que de um fiel de balança se tratasse, evoluiu para um sistema internacional caracterizado pela «complexidade, não linearidade, imprevisibilidade, heterogeneidade, mutabilidade e dinamismo» (Garcia, 2008, p. 103).

Os actores transnacionais são, na actualidade, percebidos pelos Estados de forma diferente. Ainda que não seja um fenómeno novo, a resultante do incremento das solicitações colocadas por estes actores, para além do seu alcance, transformaram os actores não-estatais numa fonte de incerteza internacional. Os grupos terroristas, por exemplo, que antes da queda do muro de Berlim era um assunto de segurança interna, passaram a desempenhar um papel central a partir do momento que foi identificado, como seu interesse, aterrorizar a população através da violência massiva[47]. Treverton refere que estes actores apresentam ausência de padrões. Classifica a sua acção como circunstancial e insere-os na categoria de mistério, onde a incapacidade de identificar as causas e os efeitos é enorme (2009, p. 18).

Em virtude das alterações operadas na ordem internacional, o período pós-guerra fria veio fazer ressaltar vários problemas ao nível da organização e gestão dos SIN (Jackson, 2005, p. 45). Durante a guerra fria as necessidades de *intelligence* sobre o inimigo originou, a Leste e a Oeste, um crescimento massivo das comunidades[48] de *intelligence*, principalmente nos EUA e

[47] Como no constante dos atentados de 11 de Setembro de 2001, nos EUA, de 12 de Janeiro de 2016, em Istambul-Turquia, de 22 de Março de 2016, em Bruxelas-Bélgica, de 18 de Janeiro de 2017, no Malí; de 29 de Janeiro de 2017, em Canadá; de 13 de Fevereiro de 2017, no Paquistão; de 3 de Abril de 2017, na Rússia; de 7 de Abril de 2017, em Estocolmo-Suécia; de 22 de Maio de 2017, em Manchester-Reino Unido, de 31 de Maio de 2017, em Cabul-Afganistão, de 2 de Junho de 2017, em Filipinas, de 2 de Março e 3 de Junho de 2017, em Londres-Inglaterra, de 7 de Junho de 2017, no Irão e; de 20 de Abril de 2017, em França.

[48] Por comunidade apresentamos o entendimento de Thomas Troy. Para aquele autor a comunidade de *intelligence* é *"the colection of those entities loosely knitted together by a number of commitees chaired by the director of Central Intelligence or his appointee. The objective of the knitting is the effective and efficient conduct of the intelligence and counterintelligence functions of the United States government"* (Troy, 2004, p.

na antiga URSS, criando constrangimentos posteriores na construção de um processo de *intelligence* racional e eficaz. Ainda que a maioria dos Estados tenha desenvolvido capacidades de *«análises de todas as fontes»*[49], mantiveram-se três factores que atrasaram o processo: o incremento avassalador das actividades de pesquisa[50] patente nas enormes quantidades de dados, sem precedentes, a requerer análise e a proliferação de agências para lidar com este problema; a dificuldade de cooperação e coordenação entre agências foi agravada em virtude da inevitável, rivalidade burocrática que, como Richard Aldrich *apud* Jackson, observa *«cada comunidade de inteligência "nacional" no oeste foi regularmente estarrecido por rancorosas brigas»*[51] (2005, p. 46); e o facto destes sistemas, desde o fim da Guerra-Fria, terem de lidar com uma série de novos desafios à segurança dos Estados, como por exemplo a proliferação de tecnologia nuclear ou o terrorismo transnacional, entre outros.

Todos estes exemplos demonstram o que Jackson designa como o *«elemento essencial de organização como um factor de limitação no uso efectivo da inteligência»*[52] (2005, p. 47), a incapacidade das estruturas se reorganizarem, por norma, de forma preemptiva. Não estando preparadas para fazer face aos novos problemas que se apresentam, ou seja, possuírem falta de flexibilidade.

Neste contexto, os Estados, independentemente do regime[53] que possuem, não diferem substancialmente uns dos outros. São hierarquizados e burocráticos procurando garantir os fins de segurança, bem-estar social e justiça, aos seus cidadãos (Treverton, 2009, p. 15). Para que tal seja possível Michael Mates *apud* Bessa sublinha que «serviços secretos fiáveis é um pré-requisito da política: sem uma avaliação objectiva das ameaças ao interesse nacional baseadas em informações seguras de um leque de fontes, os ministros sentirão a falta de uma base sólida para tomar medidas efectivas» (2001, p. 123). Demonstrando da necessidade do Estado possuir estruturas organizadas que permitam, de forma permanente e sistemática, garantir a avaliação objectiva das ameaças ao interesse nacional. Importa, pois, que os OISE possuam uma organização flexível capaz de fazer face aos desafios actuais.

---

27). Importa referir que esta noção de comunidade de *intelligence* foi publicada originalmente em 1988, antes da reestruturação que coloca o *Director of National Intelligence*, Norte-americano, com funções de coordenação.

[49] «*all-source analysis*»

[50] Em virtude da incerteza, por um lado, e do incremento avassalador da informação disponível em fontes abertas e de satélites.

[51] *«each 'national' intelligence community in the west was regularly convulsed by rancorous quarrels».*

[52] *«essencial element of organization as a limiting factor on effective use of intelligence».*

[53] Por Regime político pode-se entender "o conjunto das instituições que regulam a luta pelo poder e o seu exercício, bem como a prática dos valores que animam tais instituições" (Levi, 1998, p. 1081).

Os sistemas de *intelligence*, enquanto estruturas burocráticas, não são instrumentos passivos dos governantes. Ainda que o seu fim último[54] seja o apoio aos decisores em assuntos de segurança nacional (Gookins, 2008, pp. 65 e 66), a sua actuação tem impacto, de forma directa ou indirecta, nas instituições e no processo de decisão política. Por outro lado, decisor político também não é um recipiente passivo da *intelligence*, já que influencia todos os seus aspectos (Lowenthal, 2006, p. 2), inclusivamente a organização das estruturas, através das necessidades de informação que possui.

Ao identificar os factores de que depende o desenho organizacional dos OISE, Michael Warner (2009, pp. 26-37) identifica três vectores base: a «Grande Estratégia Nacional» (GEN), o regime e a tecnologia.

A primeira variável a ter em consideração é a GEN, que segundo Romana, deve ser «percebida e desenhada como um sistema. Mas um sistema enquanto forma de organização da decisão e execução política» (2008, p. 99), é o que Loch Johnson sublinha como sendo o ponto de partida para determinar *«…a extensão da distribuição de recursos escassos da nação para actividades de inteligência, é um claro delineamento de seus objectivos internacional e seus adversários…»*[55] (2003, p. 639). Warner decompõe a GEN em sete elementos: a orientação básica – a postura, que pode ser passiva, agressiva ou vigilante; a geopolítica – que refere as relações de poder relativamente à região e que tem influência na postura; os motivos – são os fins da política, que Bessa sistematiza como a segurança, o fim económico, a influência política, a influência cultural e a criação de imagem (2001, p. 86); os objectivos – relacionados com os motivos, que podem ser a sobrevivência ou o expansionismo, por exemplo; as fontes de apoio ou mediação – as redes de relações de um determinado Estado e podem referir-se a aliados, neutrais, competidores, etc.; situacional – que varia entre o conflito à cooperação; e a cultura estratégica – que é o contexto histórico e a percepção colectiva do mundo e das ameaças que impõe.

[54] É o que "*não está ordenado a fins ulteriores"* (Pires, 1985, p. 638).
[55] «…the extent of a nation's allocation of scarce resources for intelligence activities is a clear delineation of its international objectives and its adversaries…».

Assim, Estados com menor envolvimento externo ou ameaças podem, por exemplo, descurar a *intelligence* externa[56]. A estratégia também determina alianças e a ligação em *intelligence*, entre estruturas de Estados aliados (Warner, 2009, p. 29).

O regime político é a segunda variável. Warner analisa o regime tendo como base cinco elementos: a tipologia de soberania – se é um Estado, um quase-Estado, em império, uma cidade-Estado, etc.; a forma de governo – representativa, aristocracia ou tirania, ou seja, dependendo da forma de governo pode-se perceber a forma de exercer a fiscalização das actividades do SIN; a fiscalização – a forma de exercer a supervisão dos SIN, isto é, seja um governante, conselho de ministros, conselho de fiscalização, ou outros, dependem do tipo de governo; a estrutura ministerial/departamental – o tipo de tarefas e gabinetes criados para conduzir os destinos do Estado podem afectar o sistema que existe para os apoiar, por exemplo, a dependência do sistema pode depender da orgânica do governo; e os desafios internos – alguns Estados possuem oposição, fricção e, até conflitos internos que pode variar da resistência passiva à insurreição armada e os seus motivos podem ser vários[57] (2009, p. 30).

De acordo com Bozeman *apud* Warner (2009, p. 31), as democracias tendem a dar mais ênfase à *intelligence* externa que à interna, uma vez que, a base da democracia são os direitos, liberdades e garantias dos seus cidadãos. Nesse sentido, para Dziak *apud* Warner (2009, p. 31), as ditaduras dão maior preponderância à *intelligence* interna de forma a monitorizar potenciais instigadores contra o poder estabelecido, já que é a manutenção do poder a sua principal preocupação, edificam «*Estados contra-inteligência*»[58]. Os Estados Imperiais tendem a empenhar os esforços da *intelligence,* quer internamente quer em relação a Estados inimigos ou potencialmente inimigos.

Por fim, a tecnologia, que ao determinar os objectos da *intelligence* e os meios empregues, também produz influência nas estruturas. Assim, Warner identifica cinco elementos, na decomposição desta variável: a informação – a forma como se pesquisa, armazena, transmite e protege a informação; a produção – sugere os «alvos» do sistema, por exemplo, os esforços

[56] Lowenthal (2006, p. 12) refere que foi a ausência de interesses nacionais, para além das suas fronteiras, o factor preponderante para que os EUA se mantivessem, por cerca de 170 anos sem um SIN organizado.
[57] Diferenças de classe, credo, raça, étnicas ou ideologia, entre outras. Por exemplo, a oposição interna pode ser espontânea, isto é, «nascido» internamente ou com base externa, uma estratégia indirecta de um outro Estado.
[58] «*counterintelligence States*».

de *intelligence* direccionados a uma sociedade rebelde, baseada no trabalho «escravo», serão diferentes se o «alvo» for uma sociedade desenvolvida tecnologicamente; os recursos – disponíveis aos esforços das *intelligence*, por exemplo, energia, capital humano, etc.; as formas sociais e institucionais – a forma como a sociedade se organiza, isto é, de forma tribal, ou outras, marcam as diferenças das capacidades e necessidades de *intelligence* e; militar – a forma como o Estado aplica a violência, a organização, mobilidade, letalidade, etc., determinam as necessidades de oportunidade e relevância da *intelligence*, as capacidades analíticas e possivelmente a importância relativa dos meios de pesquisa e disseminação da *intelligence* produzida por meios humanos ou técnicos.

O factor tecnológico é, naturalmente, mais sentido por aqueles Estados que procuram manter um elevado nível tecnológico, seja por razões defensivas, seja por razões ofensivas.

Para Michael Herman (2004, pp. 4 e 5), o desenho organizacional difere de região à região, não por questões idiossincráticas, mas por causa de uma história e valores sociais partilhados. Ideia que Lowenthal deixa transparecer quando refere que *«o sistema de inteligência dos Estados Unidos continua a maior e mais influente no mundo»*[59] (2006, p. 11), em virtude de ser entendido como um modelo a seguir, um modelo rival ou, apenas, como «alvo». Herman parte da observação de características organizacionais e operacionais dos sistemas americano e britânico para de seguida explicitar que os padrões se aplicam aos diversos sistemas nacionais, através de círculos concêntricos. Assim, o núcleo é formado por EUA e Reino Unido, onde os padrões são mais intensos. Num segundo círculo, os sistemas pertencentes aos Estados da Europa Ocidental e Israel, que por possuírem uma história partilhada com os primeiros, as alianças da II Guerra Mundial, as relações militares sobre os auspícios da Organização do Tratado do Atlântico Norte (OTAN) e outros tipos de cooperação internacional, permitem possuir padrões do núcleo, *«a maioria das organizações oferecidas aqui, aplica algum grau neste círculo ocidental»*[60] (Herman, 2004, p. 5). Por fim, o círculo exterior onde se encontram os Estados comunistas e ex-comunistas onde os padrões e generalizações de Herman se fazem sentir de forma bastante ténue.

[59] *«U.S. intelligence system remains the largest and most influential in the World».*
[60] *«the most of organizations offered here, apply in some degree to this Western Circle».*

Para Lowenthal os OISE, ou «*comunidade de inteligência*»[61], são constituídos, em termos de macro-estrutura, por duas áreas funcionais: a gestão e a execução. A primeira cobre os requisitos, recursos, pesquisa e produção. A segunda abrange tarefas como o desenvolvimento dos sistemas de pesquisa, pesquisa e produção de *intelligence* e a manutenção da infraestrutura de apoio. Contudo, aquele autor acrescenta ainda que há outra função, que não sendo das mais fortes ela terá que existir, a avaliação, cuja tarefa será de relacionar os meios – recursos: financeiros e humanos – aos fins da *intelligence* – resultados: análises e operações – o que de alguma forma poderá garantir a necessária avaliação interna que suporte a flexibilização necessária para as pressões que o meio coloca nas organizações de *intelligence* (2006, p. 33 e 34).

Cepik (2003, p. 125-128) refere que, ainda que todos os sistemas de *intelligence* possuam as mesmas atribuições, diferem entre si, em termos de desenho organizacional, em virtude da forma como as escolhas estruturais, os diferentes interesses e preferências dos actores relevantes e o ambiente externo influenciam sete elementos: (*i*) o organismo de coordenação das actividades de *intelligence*; (*ii*) as agências ou organizações dedicadas à pesquisa de *intelligence* – em que, de acordo com aquele autor, as agências dedicadas à pesquisa de *Human Intelligence* (HUMINT) estão separadas das agências de *Comunications Intelligence* (COMINT) ou *Electronic Intelligence* (ELINT), por exemplo; (*iii*) as agências de análise; (*iv*) as unidades departamentais de análise das diversas agências; (*v*) os subsistemas de *intelligence* de defesa e segurança; (*vi*) os órgãos de formação e treino; (*vii*) instâncias de fiscalização externa, seja dependente do poder executivo, legislativo ou judicial.

Tendo como base algumas variáveis genéricas – tais como o grau de centralização da autoridade sobre o sistema, o grau de integração analítica da *intelligence*, a maior ou menor separação entre as funções de *intelligence* e da política e a eficácia dos elementos de supervisão externa – o autor identifica três tipologias base dos Sistemas de Informações Nacionais. O primeiro, o modelo «anglo-saxónico»[62], é caracterizado pela grande centralização das unidades do sistema, grau elevado de integração analítica, uma separação média entre *intelligence* e política e uma eficácia média nos mecanismos de supervisão. O

[61] «*intelligence community*».
[62] Inclui os EUA, o Reino Unido, Canadá, Austrália, Nova Zelândia e com algumas reservas a Índia e a África do Sul.

segundo, designa como modelo «europeu continental»[63], caracteriza-se como exercendo um grau de autoridade médio sobre as unidades do sistema, uma integração analítica média dos produtos da *intelligence*, um alto envolvimento das actividades de *intelligence* e as instâncias da decisão e, finalmente, uma eficácia baixa nos mecanismos de supervisão das actividades de *intelligence*. O terceiro e último modelo apresentado por Cepik, é aquele que o autor classifica como o modelo «asiático»[64], tem como características principais a baixa centralização da autoridade sobre as unidades do sistema, a alta integração analítica dos produtos de *intelligence*, um envolvimento médio entre as actividades de *intelligence* e as instâncias decisoras e uma eficácia muito baixa dos mecanismos de supervisão.

Em suma, os SIN, enquanto organização, são o resultado de processos específicos de criação de soluções para os desafios na área do interesse nacional. Contudo, como observam Berkowitz e Allan, citados por Komensky e Burlin, *«a comunidade de inteligência é uma burocracia clássica, caracterizada por planos centralizados, operações rotineiras e corrente hierárquico de comando. Todas estas características deixam a inteligência mal adaptada»*[65] (2004, p. 126).

Nesse sentido, é permissível inferir que a estrutura, burocrática[66], da comunidade de *intelligence* teve uma boa prestação enquanto o inimigo que perseguia era também uma burocracia[67]. Na actualidade procurar identificar intenções e movimentações de actores não-estatais – como redes terroristas, de crime organizado ou de proliferação de ADM, ou tecnologia associada – torna-se uma tarefa muito mais complexa. As características erráticas que possuem permite-lhes desafiar a necessidade de segredo e afrontar a cultura que reforça a compartimentação e isola os analistas e agências entre si (Kamensky e Burlin, 2004, p. 127), observa-se à alteração do paradigma do *need to know* – o segredo e compartimentação – para o paradigma do *need to share* – partilha de *intelligence* – o que vai induzir à necessidade de desenhos organizacionais mais ágeis e com capacidade de adaptação constante ao meio exterior, isto é, mais flexíveis.

---

[63] Inclui a Alemanha, a França, a Federação Russa, a Polónia e a Itália. Inclui, ainda com algumas reservas o Brasil e a Argentina.
[64] O autor inclui Estados como a China, o Japão, a Coreia do Sul, a Coreia do Norte, o Taiwan e com reservas a Indonésia e o Vietname.
[65] *«the intelligence community is a classic burocracy, characterized by centralized planning, routinized operations, and a hierarchical chain of command. All of these features leave the intelligence ill suited for the information age».*
[66] Avessa à mudança, por definição (Chiavenato, 2004, pp. 269-270)
[67] O Estado, o que apesar do segredo permitia vaticinar as intenções e movimentações de tal adversário.

A este propósito Amy Zegart *apud* Lewis (2003, p. 8) observa que pela sua natureza, as burocracias na área da segurança nacional, tendem a ser criadas pelo poder executivo e o seu desenho organizacional reflecte as disputas entre burocracias de segurança nacional. Para além do mais, para Zagart, citada por Cepick (2003, p. 136), as escolhas estruturais na eclosão do órgão são propensas a perdurar no tempo. A sua alteração efectua-se em virtude dos interesses do poder executivo e do ambiente externo e tenderá a ser lenta, se não for entendida enquanto uma prioridade do poder executivo. Assim, de acordo a mesma autora, os governantes estão sujeitos a constrangimentos de tempo, de conhecimento e controle das suas agendas e da necessidade de realização dos objectivos políticos.

A necessidade de obter o apoio da opinião pública não pode ser posto em causa com disputas acerca do desenho organizacional de uma burocracia, uma vez que os subsistemas de *intelligence* têm conhecimento de áreas vitais do Estado, agendas mais delimitadas dos governantes e fortes incentivos para uma participação activa no desenho organizacional. Para além do mais, em sistemas complexos e com dependências cruzadas, como é o caso da maioria dos SIN, os problemas de coordenação são outro dos factores que limita severamente a capacidade de resposta a outros utilizadores que não aqueles que estão na cadeia hierárquica, directa.

Francis Rourke *apud* Dougherty e Pfaltzgraff ao identificar a lei da inércia burocrática referia que «as burocracias imóveis tendem a permanecer imóveis e as burocracias activas tendem a reproduzir actividade» (2003, p. 708), deixando antever que as burocracias não são todas iguais já que umas apresentam uma maior resistência à mudança do que outras, ainda que para os decisores as burocracias em cujos departamentos executivos forem estimulados a desenvolver determinadas capacidades podem representar algum risco, isto é «quando as burocracias ganham importância, são muito difíceis de refrear» (Dougherty e Pfaltzgraff, 2003, p. 709), uma vez que possuem a capacidade de influenciar o curso dos acontecimentos. O seu poder depende da vontade do executivo, o governo.

1.5. O CONHECIMENTO

Para Karl Deutsh *apud* (Romana, 2004, p. 258) é necessária a existência de mecanismos de informações que, a qualquer momento contribuam para o *decisor*[68], através da produção de *decisões*[69] que equilibrem *as necessidades*[70] de âmbito interno e externo, sendo dirigidas aos diferentes sistemas de estruturação do Estado.

O ciclo de produção de informações não sofre, nem tem a capacidade de absorver o impacto externo a que todo o ciclo de informações está sujeito. Como tal, a concepção do processo de informações, permite efectuar a verificação das diferentes alterações e sujeições, a que todo o processo está sujeito, permitindo efectuar uma leitura e compreensão do que pode ser desprezível (Gill & Phythian, 2009, pp. 3-7).

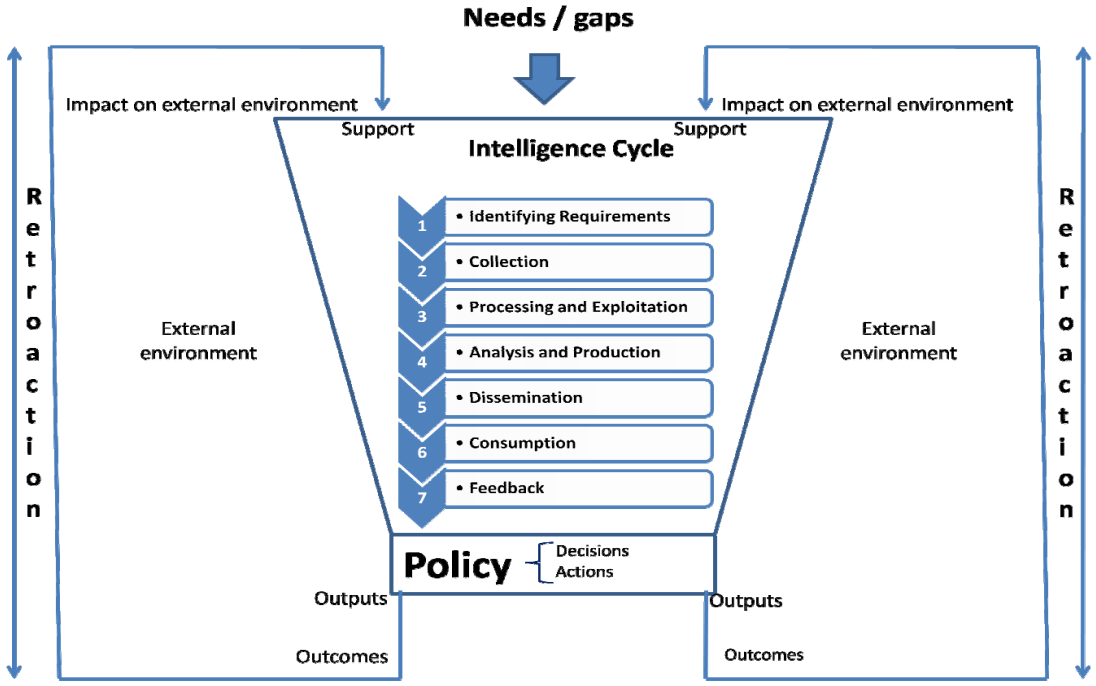


Figura 1.2 – Intelligence process[71] (Adaptação de Gill & Phitian, 2009, p. 4)

[68] *decision-making*
[69] *Outputs*
[70] *the needs*
[71] Processos de informações

De acordo com a figura 1.2, as exigências e os *gaps* são as razões identificadas, de resposta solicitada pelos decisores, com a intenção de aplicarem o produto operacional na elaboração das suas políticas. Os support caracterizam-se pelas obrigações e meios dos serviços de informações relativamente ao sistema.

Os *outputs* correspondem às decisões (Dougherty & Pfaltzgraff, 2003, p. 703) e acções com base nos *resultados*[72] dos serviços de informações. Os *outcomes* espelham os efeitos desejados, ou não, podendo influenciar o processo num sentido de retroactividade.

A alimentação do processo tem a capacidade de se alterar através da influência do ambiente exterior no qual a informação foi recolhida e a análise empreendida (Gill, 2009, pp. 86-87).

Todo o processo é dinâmico, porque para além de ser retroactivo permite uma realimentação permanente, quer no ambiente externo, quer no ambiente interno. O ciclo de produção de informações apresenta uma forma de funil, que ilustra o ponto em que se verifica que nem toda a informação recolhida é necessária, ou convertida em informações (Gill & Phythian, 2009, p. 4), justificando o afunilamento dos *outcomes*.

Pode ser visto como um funil que recebe informações, não necessariamente secretas, produzindo informações como produto final e disseminado para vários utilizadores com capacidade de decisão. Lowenthal (2003, p. 28) descreve esta situação de um modo muito simples: (i) faz-se a questão; (ii) recolhe-se a informação; e, (iii) responde-se à questão. No entanto, não ignora a possibilidade desta simplicidade sofrer alterações e distorções que alteram o resultado esperado.

Para fins de análise o ambiente deve ser dividido em ambiente interno e externo: «o primeiro abrange todos os sistemas exteriores à sociedade global em exame, com o qual está presumivelmente em relação» (Moreira, 2009, p. 117), onde se verifica a *retroaction* que processa os *outputs* desenvolvendo novas *needs* e *gaps*; o segundo compreende «todos os sistemas internos que abarcam a mesma sociedade global, designadamente os sistemas psicológico, biológico, religioso, global» (Moreira, 2009, p. 117), onde o processo de informações nunca acontece no vazio, existindo sempre um contexto pessoal ou

[72] *outcomes*

organizacional, tal como factores intrínsecos do próprio processo de informações (Gill & Phythian, 2009, p. 85).

Apesar de nem sempre se verificar, o processo de informações deve ser estanque a qualquer sistema de influência ou pressão, permitindo uma decisão política que vise o interesse do Estado e não interesses particulares. A actividade política deverá passar pelo bom senso, de acordo com as informações recebidas, com capacidade de decisão e determinação para afrontar os mais variados grupos de influência e de pressão (Carvalho, 2010, pp. 16-17).

Este processo de informações, para além de apresentar as informações como um processo interactivo, decompõe o processo de informações em fases fundamentais, apresentando diferentes finalidades em cada momento de análise do próprio processo. Permite uma interligação com sistemas exteriores, sem se deixar influenciar durante o processo, realçando os objectivos de acordo com as necessidades dos decisores através do impacto dos diferentes produtos de informações, permitindo seleccionar opções alternativas que minimizam o problema da incerteza (Dougherty & Pfaltzgraff, 2003, p. 704).

Ao definirmos este modelo, identificamos um problema conceptual neste processo de informações. Tal deve-se ao facto de utilizar apenas factores exógenos[73], sendo difícil considerar e mensurar as motivações ou preferências, as qualidades morais e, capacidades intelectuais dos decisores e dos técnicos de informações (Herman, 2004, pp. 225-226). No entanto, «quem pretenda dominar, nas melhores condições, os factores que influem nos estudos para chegar a uma decisão política, de modo a apoiar a sua execução e orientar a sua conduta, têm que dispor de um serviço de informações que trabalhe eficientemente todos os elementos disponíveis e procure obter os que se tornem necessários» (Cardoso, 2004, p. 148).

A gestão de desempenho é elaborada a partir de um resultado inesperado, quando se verifica um resultado aquém do esperado. Os padrões de desempenho são definidos por uma unidade de comportamento, directamente relacionado com a dinâmica da estação e pela forma como está estruturada. Mesmo quando há *inputs* e *outputs* identificáveis e referenciáveis, o processo de decisão está envolvido em mistério, característica das próprias informações, tal como uma *caixa preta*, sem nenhuma indicação envolvente nem do seu circuito interno (Herman, 2009, pp. 140-142).

[73] Estes factores exógenos podem ser de âmbito político, estratégicos, económicos, geopolíticos, entre outros.

As componentes essenciais do processo de informações são enfatizadas, pela recolha por meios humanos e técnicos, na qual se visualiza uma certa importância dos técnicos de informações operarem próximos dos decisores, o que diminui a influência externa no tratamento e análise (Herman, 2009, p. 56). A rotação dos técnicos de informações e sua gestão só se justificam, quando ocorrem desvios negativos dos resultados face aos objectivos fixados, de modo a corrigir o seu desempenho.

Outra forma de equacionar a *intelligence* é enquanto processo, pelo qual, determinados tipos de informações são requeridos[74], coligidos, analisados e disseminados, bem como, determinados tipos de acções cobertas são concebidos e conduzidos.

Este processo também designado como «ciclo de produção de informações» procura espelhar um processo cíclico que envolve um conjunto de etapas, repetidos e interdependentes, cujo objectivo será o de adicionar valor-acrescentado[75] aos *inputs* iniciais de modo a obter um produto substancialmente transformado e talhado às necessidades dos decisores. O ciclo de produção de informações operacionaliza «*o processo de descobrimento de segredos pelos meios secretos*»[76] (Waltz, 2003, p. 2). Isto é, poderá ser entendido como o processo de gerar conhecimento necessário para alimentar o processo de decisão, processando os dados, de forma sistemática de modo a gerar o conhecimento necessário aos decisores.

1.5.1. O ciclo de produção de informações

Segundo Johnston (2005, p. 45), a produção de informações é representada convencionalmente por um modelo designado por "ciclo de produção de informações".

Dependendo dos técnicos de informações, investigadores ou professores, existem vários modelos (quatro, cinco, seis e sete fases). Mas, todos eles têm um fim em comum – a transformação de *matéria-prima*[77] num produto final apropriado à tomada de decisão.

O ciclo de produção de informações visa a eficácia e eficiência, não só na forma como emprega os meios tecnológicos, como na verificação da rentabilização dos técnicos de

[74] Por identificar requisitos significa, para Mark Lownthal, "defining those policy issues or areas which intelligence is expected to make a contribution, as well as decisions as to which of these issues has priorities over others*"* (2006, p. 54).
[75] Amanda J. Gookins, a este propósito, sublinha que "the intelligence analyst turns information into intelligence by connecting data to issues of national security, thereby giving them value" (2008, p. 66)
[76] «*the process of the discovery of secrets by secret means*».
[77] *raw material*

informações de uma forma assertiva, proporcionando um produto prospectivo no momento mais adequado (Johnston, 2005, pp. 45-46).

Os produtos de informações são destinados a vários níveis de utilização das mesmas: os técnicos de informações iniciam a sua actividade após indicações dadas pelos decisores acerca das necessidades, prazos de obtenção e prioridades de informações necessárias (Lowenthal, 2003, pp. 41-42).

Os mecanismos de informações podem produzir informações, destinadas a vários níveis de utilização das mesmas. A pesquisa e recolha de informação, com o respectivo tratamento e análise, permitem adquirir nítida vantagem perante um determinado adversário ou oponente.

Os decisores nem sempre têm a possibilidade de coordenar com os técnicos de informações as suas necessidades e prioridades de informação. Como tal, os técnicos de informações utilizam um conjunto de ferramentas organizacionais e analíticas para completar, detalhar e priorizar as exigências (Johnston, 2005, p. 47).

Os técnicos de informações criam modelos e cenários, que permitem a um decisor, planear com antecipação, conferindo-lhe consistência nas suas decisões.

O ciclo de produção de informações refere-se a várias fases do processo de transformação de notícias e informação em informações, em que o decisor percebe a necessidade de uma determinada informação e solicita o trabalho dos serviços de informações para produzirem um produto analítico que esclareça as necessidades em causa (Herman, 2009, p. 286).

O processo que seleccionamos emprega a aproximação de sistemas e simulações que permitem criar cenários semelhantes, ou mesmo reais, minimizando as negligências.

O modelo apresentado, figura 1.3, é de sete fases: *Identificação dos requisitos*[78]*; recolha*[79]*; processamento e exploração*[80]*; análise e produção*[81]*; disseminação*[82]*; consumo*[83]*; e*

[78] *identifying requirements*
[79] *collection*
[80] *processing and exploitation*
[81] *analysis and production*
[82] *dissemination*
[83] *consumption*

retroalimentação[84] (Lowenthal, 2003, pp. 41-50).

a) Identificação dos requisitos

Cada Estado tem o seu próprio sistema de segurança, tal como os seus interesses de política externa. Mas o meio internacional é de reajustamentos dinâmicos e fluidos, ocasionais de prioridades e é mesmo provável entre os interesses chave, de acordo com as necessidades, num dado sistema dinâmico, com as eventuais *gaps*, as prioridades de informações devem reflectir sobre as prioridades da política e não sobre a comunidade de informações.

Por vezes as necessidades são óbvias, em que não se torna necessário efectuar qualquer discussão sobre a sua determinação, no entanto, enquanto os decisores não adoptam a sua decisão final, o sistema flui e tudo se movimenta, o que implica a redefinição urgente das definições de prioridades (Lowenthal, 2003, p. 43).

A definição de prioridades consiste no planeamento de recolha para uma possível base de dados, sendo a chave para se verificar o início do ciclo de produção de informações. A avaliação do planeamento efectivo da base de dados existente, deve assegurar uma informação adicional a fim de preencher qualquer *gap* existente nos ficheiros das bases de dados existentes.

Define os requisitos de informações, prepara o plano de pesquisa, emite ordens e pedidos de pesquisa para os órgãos respectivos, e verificar permanentemente a produtividade da pesquisa.

No entanto, se uma necessidade, ou *gap*, não for satisfeita com os actuais sistemas de recolha, poderá, através do desenvolvimento de sistemas técnicos próprios para a situação ou através de fontes humanas. Tal satisfação não será imediata e levará o seu tempo. Assim, a incerteza sobre o solicitado para a recolha, só fará com que o processo de produção de informações se torne moroso logo desde o início (Lowenthal, 2003, p. 45).

[84] *feedback*

b) Recolha

Refere-se a recolha de *matéria-prima* que se destina a satisfazer as necessidades e *lacunas*. Estes dados podem ser derivados de qualquer tipo de fontes, sejam elas abertas ou fechadas (secretas), derivando directamente dos *requisitos*. É talvez o primeiro passo, onde os recursos das informações entram em acção (Lowenthal, 2003, p. 45), utiliza os meios na recolha de informação para posterior transformação em produto trabalhado.

Esta fase pode abranger e aplicar vários métodos, ou somente um, desde o emprego de técnicas e meios tecnológico às fontes humanas. Nenhum destes métodos consegue providenciar ou garantir um entendimento total de determinadas situações específicas, no entanto, alguns serviços de informações usam os mais variados métodos possíveis, permitindo a validação da informação, minimizando o erro de análise, na perspectiva de se atingir a precisão (Hannah, O' Brien, & Rathmell, 2005, p. 5).

Segundo (Gill & Phythian, 2009, p. 31) a informação é recolhida de acordo com dois modos de actuação distintos: (i) recolha com base em documentação de fácil acesso e disponível a qualquer interessado (aberta); e, (ii) aplicação de técnicas mais agressivas, tal como a infiltração clandestina em determinadas áreas com o intuito de recolher informação (*acção coberta).*

Sem recolha, as informações não são mais do que simples adivinhação, é necessário obter a informação necessária à satisfação dos requisitos de informações e fornecê-los aos sectores de processamento e de produção. A recolha de dados é o trabalho mais intenso em termos de acumulação de trabalho no ciclo de produção de informações. Normalmente, é a fase com maior ênfase no ciclo de produção de informações, com as leis e modos de emprego dos serviços e agentes, com dedicação significativa no trabalho e com as fontes a efectuarem a recolha e acumulação de *matéria-prima*. Onde, a actual tecnologia e o suporte legislativo dos serviços de informações facilitam, e em muito, o trabalho nesta fase (Peterson, 2005, p. 6).

c) Processamento e exploração

Refere-se à conversão de dados para um formato de possível análise, permitindo converter a informação recolhida num produto adequado à produção de informações (Hannah, O' Brien, & Rathmell, 2005, p. 6). A transformação de informação recolhida em formatos perceptíveis é conhecida por *processing*, onde os sinais complexos e codificados devem ser transformados e

decifrados em informação perceptível. Depois de transformados devem ser aproveitados para posterior *exploitation*, através da análise, convertendo a informação em informações (Lowenthal, 2003, p. 46).

Esta fase permite transformar o material recolhido em produtos exequíveis de futura utilização e emprego, relegando o material irrelevante, detectando mesmo informação incorrecta, colocando o *raw material* numa ordem de sequência lógica. O desenho da base de dados é uma tarefa crítica para o retorno e validação da informação. O recurso a empresas de *software* permite desenvolver produtos que permitem minimizar esta situação. Serviços de informações menos ricos geralmente usam o *off the shelf software* para reduzir os custos. Actualmente, a tecnologia existente permite a utilização de diferentes bases de dados a fim de interagir através dos dados recolhidos com as bases de dados já existentes (Peterson, 2005, p. 7).

d) Análise e produção

Descreve o processo de conversão de dados em informações propriamente ditas, com verificação do grau de confiança e verossimilhança. Permite converter a informação em informações, através da integração, avaliação, análise e interpretação de todos os dados disponíveis, complementadas pela preparação dos produtos finais, de acordo com os requisitos fixados pelos decisores. Na recepção da informação recolhida e sua transformação, os processos analíticos[85] permitem efectuar uma leitura com maior precisão, identificando a presença, ou falta, de factos e evidências nos cenários em causa (Peterson, 2005, p. 7), os analistas que através das suas análises produzem produtos de informações que vão auxiliar os decisores no processo de decisão (Hannah, O' Brien, & Rathmell, 2005, p. 6).

Nesta fase podemos ter dois tipos de análise: (i) sistemático dos elementos do processo, em que os resultados podem ser o esperado; e, (ii) aproximação sistémica, que identifica as relações dos elementos participantes no processo e a influência entre eles (Johnston, 2005, p. 46).

[85] Existem várias "ferramentas" analíticas de apoio à análise, tais como: diagrama de ligação, matriz de associação, tabela de eventos, entre outras.

e) Disseminação

É a audiência intencional, efectua a distribuição das informações aos decisores em formato apropriado, tendo a necessidade e a responsabilidade de usar as informações para divulgação a quem de direito, respeitando o princípio da necessidade de saber (Peterson, 2005, p. 7).

É necessário ajustar os produtos de informações à forma como pretendem transmitir os seus resultados aos decisores, tais como: brifingues, relatórios, etc. (Hannah, O' Brien, & Rathmell, 2005, p. 6).

f) Consumo

Nesta fase as informações estão ao dispor dos decisores para sua utilização e emprego. São utilizados uma grande variedade de produtos, em diferentes formatos, com diferentes graus de detalhe, para uma ampla e vasta gama de decisores. Alguns serviços de informações optam por não utilizar esta fase, porque afirmam que o produto de informações está completo, acabado e entregue aos decisores (Lowenthal, 2003, p. 49). Para a importância do *consuptiom* importa referir que somente nesta fase é que se verifica o consumo do resultado final, no *raw material* transformado em produto final, em informações (conhecimento).

g) Retroalimentação

Esta fase materializa a verificação dos produtos de informações e a sua efectivação. Parte desta informação é proveniente dos decisores. Para se assegurar se o produto conseguiu satisfazer as necessidades dos decisores, a forma de *feedback* deverá especificar determinadas considerações que permitam efectuar uma leitura de satisfação, ou não, no uso e emprego dos produtos de informações (Peterson, 2005, p. 7).

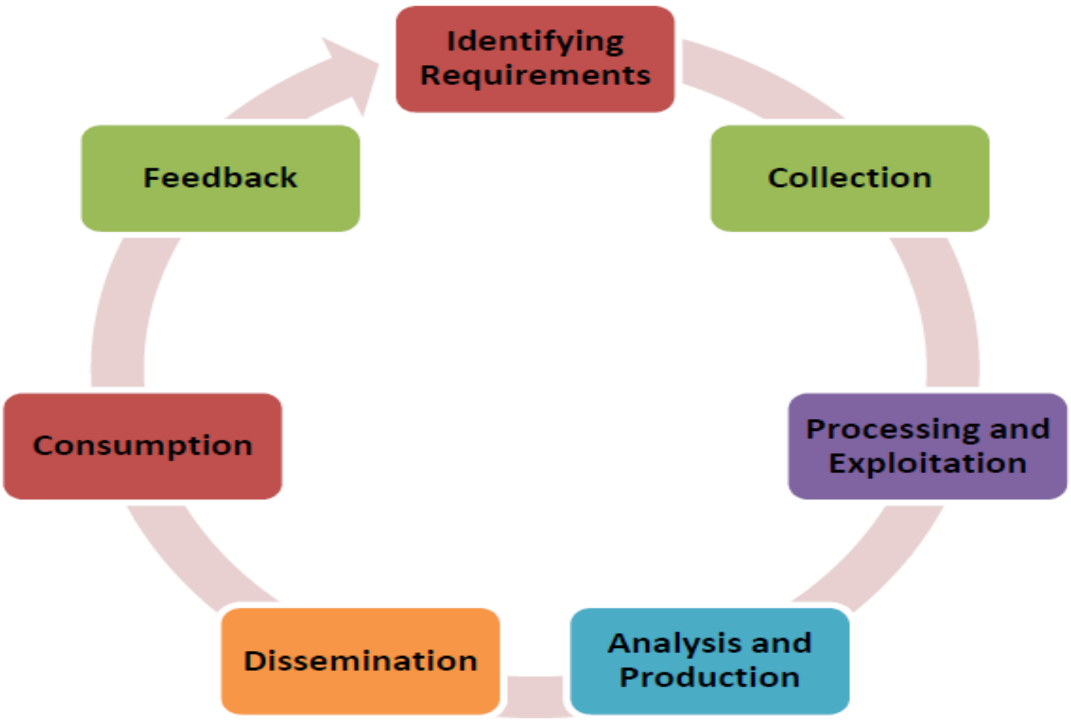


Figura 1.3 - Ciclo de produção de informações (Lowenthal, 2003, p. 41)

O processo utilizado para a sua obtenção, em termos conceptuais, é idêntico a qualquer que seja o nível e o tipo de informações a obter. O ciclo de produção de informações é um modelo unidimensional e unidireccional para cada necessidade ou *gap* (Hannah, O' Brien, & Rathmell, 2005, p. 4), porque opera numa única dimensão e numa direcção uniforme de fase em fase.

Normalmente, pensa-se, o enfoque está na recolha de informação, mas a maioria dos fracassos é devido à principal tarefa das informações estratégicas, à inadequada análise ou a outros motivos exteriores ao ciclo de produção de informações. O decisor corre o risco de trabalhar com informação corrente em vez de informações. Daí, a necessidade de um ciclo de produção de informações, que permita seleccionar o que se pretende ter, a capacidade e o *Know how* para trabalhar o *raw material* desde a sua recolha até ao produto final (Herman, 2009, p. 285).

O início do ciclo verifica-se com uma questão colocada por um decisor onde são identificados e determinados os requisitos e necessidades. É materializado, pela identificação do problema estratégico a partir de uma dada questão, sempre que um decisor necessita obter informações sobre determinado assunto, tema ou área.

É um processo dinâmico e contínuo devido ao surgimento de novos *needs* e *gaps* (Hedley, 2009, p. 213), mas não despreza nenhum produto recolhido.

Para Lowenthal (2003, p. 42), a informação trabalhada, já como informações, deve ser disseminada ao decisor num relatório escrito ou sob outra forma de difusão. É, nesta fase de transição, que aparecem novas necessidades e requisitos, permitindo uma enérgica actividade em permanente mutação, e se inicie ou se passe para uma outra fase.

1.5.2. Pesquisa centrada no alvo

O modelo de *pesquisa centrada no alvo*, figura 1.4, é característico do sistema *pulling*[86] em vez do *pushing*[87]. É utilizado na análise de geometria de objectivos que exige a participação do decisor. Neste modelo, os serviços de informações preocupam-se com as necessidades da missão, apoiando e acautelando os decisores em relação à sua acção, sem produzirem necessariamente produtos durante a análise. Permite efectuar a verificação dos resultados a qualquer momento, pela sua verificação de *lacunas* ou novos requisitos, aliados às fontes de recolha e pesquisa que geram nova informação no sistema[88] alvo. Esta abordagem permite uma maior rapidez de análise, uma vez que opera em permanente avaliação do cenário determinado [na figura 1.4 é designado por «alvo»], com recurso a uma constante base de dados e uma interligação bastante próxima entre técnicos de informações e decisores (Duvenage, 2010, pp. 12-14).

Este modelo sistémico visa a construção de uma imagem do alvo em estudo e análise, da qual todos os participantes podem extrair os elementos necessários para a satisfação das suas necessidades, permitindo uma melhor compreensão dos novos desafios. Deste modo, todos podem contribuir, em qualquer momento, de modo a criar uma imagem do alvo mais precisa (Clark, 2007, pp. 13-15).

[86] Verifica-se a utilização de produtos duma forma interactiva, mas não iterativa, empregam os produtos já fornecidos para desencadear o apoio a uma decisão.
[87] Verifica-se a utilização de produtos duma forma interactiva e iterativa, verifica–se o emprego do analista operacional, conciliando a recolha com a própria análise.
[88] Perante as actuais ameaças, o alvo deve ser analisado como um sistema complexo, porque envolve: (i) uma estrutura, definida pelos seus componentes e suas relações; (ii) uma função, caracteriza os efeitos ou resultados que o sistema produz; e, (iii) um processo, que se refere à sequência de eventos ou actividades que os efeitos ou resultados produzem (Clark, 2007, p. 17).

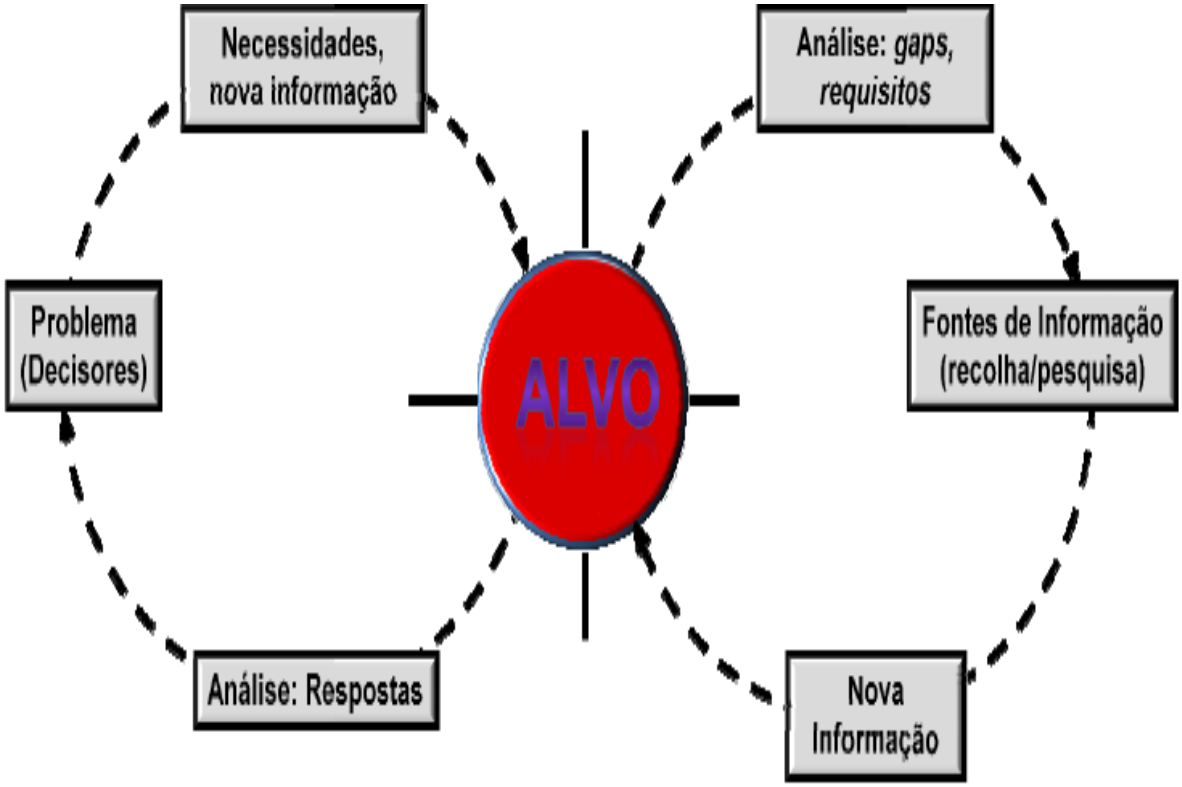


Figura 1.4 - *Target centric approach*[89] (Adaptação de Clark, 2007, p. 14).

"O Senhor falou a Moisés: «Manda homens para explorar a terra de Canaã, que Eu hei-de dar aos filhos de Israel» (...) Moisés enviou-os a explorar a terra de Canaã e disse-lhes: «Subi o Négueb, subi a montanha. Vede que terra é essa e que povo habita nela, se é forte ou fraco, pouco ou muito numeroso (...) Que cidades habita, abertas ou fortificadas?» "

Nm 13, 1-23[90]

[89] Abordagem centralizada.
[90] Livro dos Números in Bíblia Sagrada (1998).

1.6. FUNÇÕES DA INTELIGÊNCIA

Com a desintegração do «Bloco do Leste» e o recrudescimento de determinados desafios[91] surgem novas prioridades no quadro da segurança dos Estados, patentes na alteração significativa da natureza dos requisitos de *intelligence*. Assim, contrariamente aos conflitos entre Estados, maioritariamente militares, onde havia um inimigo declarado, surgem inimigos sem rosto que operam, em grupo ou isoladamente, *«especialmente obscuro, organizacionalmente flexível e muitas vezes opaco»*[92] (Ellis, 2010, p. 2). Desde o fim da guerra fria a instabilidade provocada por estes fenómenos veio expandir as fronteiras das áreas de interesse do Estado de forma avassaladora, numa lógica que sugere que a complexidade, relativamente às actividades desenvolvidas pelos OISE, tenha aumentado em igual proporção.

O paradigma da *intelligence* resultante da guerra-fria era centrado essencialmente nos Estados, que por definição, para além de território têm também população e órgãos de decisão[93]. Nesse sentido, podemos inferir que, os Estados apresentam padrões verificáveis ao longo do tempo (a história), são geográficos e burocráticos o que, em certa medida, oferece alguma previsibilidade nas suas acções. Por outro lado, a interacção entre Estados opositores era relativa; procurava-se influenciar o oponente com determinadas políticas, ou seja, esperava-se uma reacção, a qual nem sempre seria visível[94]. Em terceiro lugar, os decisores que necessitavam da *intelligence* estavam identificados como sendo os decisores políticos e militares, ainda que a informação disponível fosse parca e assentasse, fundamentalmente, em fontes secretas.

O principal «alvo» das actividades da *intelligence* ocidental era a URSS e os seus Estados satélites, cujo regime fechado limitava a informação em fontes abertas. Em quarto lugar, o produto da *intelligence* assentava no que Gregory Treverton designa de *puzzles*[95], em

[91] Como o terrorismo internacional, a proliferação de ADM, o narcotráfico, as ameaças económicas, ameaças à saúde e ambiente, entre outros.
[92] «spacialy obscure, organizationally fluid, and often opaque».
[93] Para o Professor Marcello Caetano o Estado é "um povo fixado num território de que é senhor, no interior de cujas fronteiras institui, por autoridade própria, órgãos que elaboram as leis necessárias à vida colectiva e impõe a sua execução". (Caetano, 1967, p. 117).
[94] Veja-se por exemplo, a competição nuclear entre EUA e URSS, na qual o desafio era o de perceber qual a provável modalidade de acção dos contendores e não a calibração da influência de outras nações nessa modalidade.
[95] *Puzzles* são questões a que se pode dar resposta com algum grau de certeza tendo como recurso a informação, em princípio, disponível. Isto é, consegue encontrar-se uma relação de causa-efeito. O desafio está, de acordo com Treverton, em categorizar corretamente o problema, encontrar a informação necessária e aplicar as fórmulas

contraponto aos mistérios[96] – uma vez que se procurava aceder a informação acerca das capacidades[97]. Esse produto enformava as «peças adicionais» para preencher o «mosaico da informação». Em quinto lugar, a estratégia dominante durante a guerra fria assentava na dissuasão, que para Treverton (2009, p. 37) era ancorada na ideia de que, para além das diferenças ideológicas, a URSS e os EUA eram ambos modernos, racionais e não auto-destrutivos. As intenções soviéticas eram percebidas como hostis, mas racionais. A partir do momento que Moscovo passou a deter ADM a forma de garantir de que estas não eram usadas foi através da estratégia de dissuasão[98]. Para aquele autor a *intelligence* teve um papel importante, ainda que não tenha sido vital. As necessidades de *intelligence* centravam-se nas capacidades[99] e nas intenções e percepções[100].

Após o colapso do bloco soviético os Estados ainda se colocam como oponentes aos seus semelhantes[101], no entanto com o segundo milénio surgiram outros «alvos». São os actores transnacionais que variam desde grupos terroristas, a negócios internacionais.

Se os Estados podem ser caracterizados, de acordo com Treverton (2009, p. 16) em Estados fechados[102], Estados mistos[103] e Estados abertos[104] os segundos são aqueles que vêm pressionar, com mais veemência, as alterações ao paradigma da *intelligence.* Assim, em primeiro lugar, estes «alvos» não são geográficos, muitas vezes[105] não têm uma hierarquia

---

aceites (2009, p. 17).

[96] Para Treverton (2009, p. 146), mistérios são questões que nenhuma evidência pode responder de forma definitiva. São tipicamente acerca de pessoas, e não de bens materiais. São contingenciais. Por exemplo, a taxa de inflação da Zona Euro para 2019, é um exemplo do que é um mistério, seguindo a lógica daquele autor.

[97] Capacidade é a "possibilidade de um país ou coligação de países executarem determinado tipo de acções" (Ribeiro, 2008, p. 32). A possibilidade que o autor nos refere traduz-se em meios humanos, financeiros e materiais. São estes meios que garantirão a determinado Estado ou coligação as condições que possibilitam atingir objectivos e salvaguardar interesses.

[98] A propósito das decisões racionais veja-se, por exemplo, o resultado da crise dos mísseis de Cuba, em 1962.

[99] Como por exemplo a quantidade de ogivas que Moscovo possuía, numa perspectiva de perceber de que forma as capacidades nucleares eram uma ameaça para os EUA e aliados da NATO.

[100] Como por exemplo qual era o risco que a liderança política soviética estava disposta a correr em caso de guerra nuclear.

[101] Mantendo-se como «alvos» das estruturas de *intelligence*.

[102] O caso da Coreia do Norte, por exemplo, cujas capacidades básicas se mantem secretas, sendo que a *intelligence* se foca em puzzles, e as fontes da pesquisa são secretas, uma vez que por definição, num regime fechado, a informação é em pouca monta.

[103] Como o caso da China e Irão, por exemplo, cujos puzzles se mantem, relativamente às capacidades, mas os mistérios ganham importância – as fontes secretas são importantes, mas as fontes abertas ganham uma dimensão maior que os anteriores.

[104] O caso dos Estados Ocidentais, por exemplo, cujas capacidades são transparentes e os mistérios ganham uma dimensão avassaladora – as fontes secretas têm menos valor que nos Estados anteriores, sendo o problema maior a quantidade grande de informação.

[105] Principalmente os actores relacionados com actividades criminosas (grupos terroristas, grupos de tráfico de droga, entre outros), ainda que grupos económicos transnacionais, por exemplo, não tenham a mesma estrutura

definida e não são, por norma, burocráticos. São desterritorializados e não se consegue identificar um padrão de actuação, o que origina a falta ou ausência de contexto. Em segundo lugar, há uma interacção grande entre o Estado e esta teologia de «alvos»[106]. Em terceiro lugar, os «alvos» não-estatais estão menos limitados. A falta de constrangimentos garante a necessária liberdade de acção para desenvolver determinadas actividades[107]. Em quarto lugar, desde que o mundo despertou para os fenómenos colocados por «alvos» transnacionais, os consumidores de *intelligence* deixaram de ser, apenas, os decisores políticos e militares[108].

Em quinto lugar, em virtude da natureza transnacional dos «alvos» os SIN encontram-se confrontados com uma miríade de informação que contrasta com a nitidez da informação, ainda que em muito menor quantidade, própria dos tempos da guerra fria. Pelo que separar a informação de «ruído» é, na actualidade, uma tarefa de grande monta.

Em sexto lugar, os «alvos» transnacionais envolvem *puzzles* e mistérios, mas envolvem, também, aquilo que Treverton (2009, p. 33) designa de complexidades[109]. *«Grande número de actores relativamente pequenos responde para desvios conjuntos de actores de situação. Além disso, porque interações reflectem circunstâncias únicas, eles não necessariamente repetem em algum padrão estabelecido e não são submissos para análises profética na mesma maneira como mistérios»*[110] (2009, p. 146). Em sétimo lugar, a estratégia deixou de estar associada à dissuasão, está associada à prevenção. Nesse sentido, as necessidades de *intelligence* deixam de ser importantes, passam a ser vitais. Tal como na dissuasão a lógica da prevenção é evitar o confronto, contudo, tal só é possível se os «alvos» forem sujeitos à disrupção ou se evitar que acedam às vulnerabilidades do objectivo eleito. Para tal, é necessário que os SIN tenham uma compreensão bastante apurada das ameaças em tempo.

---

dos Estados ou hierarquia. Se o padrão de comparação é o Estado, então, parece-nos adequado referir que estes actores também não são burocráticos e hierárquicos.

[106] Os grupos terroristas, por exemplo, alteram as suas capacidades em função das vulnerabilidades do seu objectivo, o que, em termos de intelligence, torna a dimensão externa e interna transversais, ao invés da estanquicidade, própria do paradigma bipolar.

[107] Por exemplo, actividades financeiras – muitas empresas transnacionais possuem orçamentos que ultrapassam os governos, tornando-se interlocutores de peso nos mercados financeiros internacionais – ou atentados que produzem vítimas em massa.

[108] A título de exemplo Treverton refere que "an aiport security officer or a public health doctor may have a more urgent «need to know» about a threat than the president of the United States because he or she may be in a more immediate position to thwart it" (2009, p. 29).

[109] Complexidades são designadas por Treverton (2009, p. 146) como mistérios-mais. Envolvem uma série de causas e efeitos que podem interagir numa variedade grande de maneiras, de forma contingencial.

[110] *«Large numbers of relatively small actors respond to a shifting set of situational actors. Moreover, because interactions reflect unique circumstances, they do not necessarily repeat in any established pattern and are thus not amenable to predictive analysis in the same way as mysteries».*

Fruto dos desafios que o ambiente coloca, estruturas de *intelligence* têm de desenvolver actividades de modo a garantir que o conhecimento é gerado, tendo em vista o necessário valor-acrescentado para a tomada de decisão e é assegurada a necessária segurança, seja nos processos, fontes, necessidades ou outros. Nesse sentido, seguindo a abordagem holística a que nos propusemos, importa tratar aqueles que Shulsky e Schmitt designam de elementos da *intelligence*. São as funções[111]: pesquisa, análise, *contra-inteligência*[112] e acção coberta. Contudo, Boraz e Bruneau (2006, p. 30) alertam para o facto de que, ainda que as quatro funções definam a ancoragem no qual o problema das informações deve ser entendido, nem todos os Estados têm a necessidade, o querer ou a capacidade de possuir vastas capacidades em todas as funções, no entanto, quase todos os Estados conduzem, pelo menos, algumas actividades de informações detendo, para o efeito, alguma organização de informações.

As duas primeiras são entendidas numa lógica de geração de conhecimento. As restantes são percebidas numa perspectiva de protecção e disrupção das actividades, capacidades e intenções, de forma a negar o conhecimento necessário para alimentar o processo de decisão do adversário.

1.6.1. A pesquisa

As capacidades de pesquisa da maioria dos Estados ocidentais tem como base toda uma miríade de meios[113] desenvolvidos durante o período da guerra fria, de forma a dar resposta às dificuldades de penetração na URSS[114] cujos principais alvos eram de cariz militar. No entanto, apesar das alterações significativas no objecto da pesquisa de *intelligence*, esta função mantém-se como uma actividade fundamental para a geração de conhecimento. É, por norma, entendida como a pedra basilar da *intelligence*. É através desta que se acede aos dados acerca das actividades, capacidades e intenções do adversário que permitem acrescentar valor à informação.

Nesse sentido, a função pesquisa[115] utiliza vários métodos[116] ou disciplinas, as quais podem ser sistematizadas, de acordo com Shulsky e Schmitt, em pesquisa com recursos a meios

[111] Entendemos função na sua acepção fundamental que, de acordo com Morujão (1985, p. 768), corresponde a operação.
[112] *Counterintelligence*
[113] Principalmente técnicos.
[114] Uma sociedade fechada com uma grande vastidão de massa terrestre, más condições meteorológicas e uma longa tradição de secretismo e decepção.
[115] A pesquisa, segundo Lowenthal (2006, p. 68) cobre três tipos diferentes de actividades: a *Intelligence* (termo

técnicos (TECHINT), humanos (HUMINT) e à fontes abertas (OSINT) (Shulsky e Schmitt, 2002, p. 11).

Cada um destes métodos de pesquisa, de acordo com Lowenthal, apresenta vantagens e inconvenientes, no entanto quando se faz a avaliação dos mesmos será importante recordar que o objectivo será envolver o máximo de métodos possíveis, principalmente em situações de maior premência para o decisor. Esta postura permitirá, porventura, a sinergia que compensa as insuficiências e desvantagens que cada uma apresenta (Lowenthal, 2006, p. 79).

A primeira, a TECHINT, possui algumas vantagens comuns, para além daquelas que cada um dos seus elementos (IMINT, SIGINT e MASINT) apresenta, não deixando, no entanto, de serem complementares. Primeiro, permite a operação remota dos sensores que utiliza, não colocando, por isso, em perigo a vida de humanos e tornando, ainda, as intenções dos decisores menos «visíveis» a possíveis adversários. Depois, são métodos, principalmente a IMINT e SIGINT, que podem com mais facilidade adquirir alvos com grande volume, como as actividades de forças militares (Lowenthal, 2006, pp. 79-94).

Individualmente, a IMINT oferece como principais vantagens o facto de ser gráfica e cativante e de fácil interpretação (Lowenthal, 2006, pp. 83-84).

A SIGINT tem como principal vantagem o acesso a planos e intenções do adversário, através da exploração e intercepção das comunicações. Permite, em última análise, ler *«o outro lado da mente, uma meta que não pode ser alcançado por imagens»*[117] (Lowenthal, 2006, p. 90), à distância. Para além de aceder a uma grande quantidade de dados, obtidos pela exploração das comunicações. No mundo globalizado os meios de comunicação incrementaram enormemente[118] pelo que é possível utilizar sistemas de intercepção da tipologia *echalon*[119],

genérico para a pesquisa); a vigilância (a observação sistemática de uma alvo – área ou grupo – por um período de tempo, geralmente alargado) e; reconhecimento (missões para adquirir informação acerca de um alvo, por vezes designa uma empresa única no tempo).

[116] Que se pode entender como um "conjunto de procedimentos e de regras para se chegar ao resultado desejado" (Russ, 2000, p. 198).

[117] *«the other side's mind, a goal that cannot be achieved by imagery»*.

[118] Telefones, telefones móveis, faxes, e-mails ou tecnologia VoIP (*Voice-over-Internet-Protocol* – permite a utilização de telefones via internet).

[119] Sistema de intercepção de comunicações global operado "by means of cooperation proportionate to their capabilities among the USA, the UK, Canada, Australia and New Zealand under the UK-USA Agreement…" (Schmid, 2001).

em que o acesso à informação, com provável valor de intercepção, se faz com recurso a pesquisas por palavras-chave (Lowenthal, 2006, p. 91).

A MASINT centra-se essencialmente no que concerne a actividades industriais e desenvolvimento de armamento. Identifica tipos de gases ou resíduos fabris – o que poderá ser de capital importância na detecção de ADM, concretamente o armamento químico – para além de identificar características específicas[120] de sistemas de armas (Lowenthal, 2006, p. 93). É neste contexto que apresenta as suas vantagens, principalmente numa época em que a proliferação de ADM, o controlo de armamento, os problemas ambientais e o narcotráfico, são algumas das principais preocupações em termos de segurança.

Contudo, a TECHINT apresenta algumas desvantagens. O facto de necessitar de sensores tecnologicamente desenvolvidos, principalmente aqueles que dependem de satélites, torna esta actividade muito dispendiosa. Para além do mais, a dependência de satélites impõe alguma falta de flexibilidade para o emprego dos sensores que deles dependem para operar, já que aquelas plataformas são programadas para operar em determinadas órbitas fixas.

Individualmente os seus elementos apresentam algumas desvantagens, sendo os aspectos operativos aqueles que entram em maior monta.

A IMINT é um método estático, isto é, é literalmente um fotograma de um determinado momento *te conta o que tem acontecido*. Em segundo lugar, está dependente das condições meteorológicas. Em terceiro lugar, as ameaças colocadas por pequenos grupos, pelas suas características[121], deixam uma «pegada» muito menor que qualquer actividade militar, pelo que só é possível empenhar a IMINT tendo como «alvo» situações em que seja visível a actividade da ameaça[122] (Lowenthal, 2006, p. 91).

A SIGINT, para além dos meios necessários à intercepção, carece de meios para a desencriptação, seja do sinal seja do conteúdo da comunicação, uma vez que é expectável que a comunicação por meios electrónicos se efectue num ambiente seguro. Em segundo lugar,

[120] Composição e material
[121] As células são mais pequenas, menos elaboradas e possuem menos visibilidade que os alvos politico-militares tradicionais.
[122] Como por exemplo, as infraestruturas de treino.

está dependente da manifestação de comunicações, já que se existir silêncio[123], torna-se totalmente ineficaz.

O segundo método de pesquisa, a HUMINT, possui como principal vantagem, o facto de garantir o acesso mais facilitado às intenções e planos de adversários, o que permite a identificação de oportunidades *«para influenciar aquele governo por informações falsas ou enganadoras»*[124] (Lowenthal, 2006: 97). Além do que, se comparada com a TECHINT, é menos onerosa[125], o que alimenta a convicção que na guerra contra o terrorismo a HUMINT é o método de pesquisa privilegiado (Lowenthal, 2006, pp. 96-97). Para além do mais, garante flexibilidade a outros métodos de pesquisa. Pode providenciar o alerta de que algo poderá ocorrer em determinada região, facilitar a interpretação dos dados colhidos por outro método ou pelo acesso a determinados «alvos» pode servir de sensor para a colocação de sensores de SIGINT, junto a alvos humanos (Lowenthal, 2006, p. 97).

Em contrapartida, este método apresenta algumas desvantagens operativas. Porque requer a proximidade ao «alvo» é confrontado com capacidades de *counterintelligence* do adversário, o que induz a um risco mais elevado em termos de vida humana e de consequências políticas, decorrentes de ganhos de informação falsa ou enganadora[126], menos passível de ocorrer quando da utilização da TECHINT. É, igualmente, um método pouco flexível[127] e moroso[128].

Contudo nem todas as fontes carecem de um processo de recrutamento tão moroso. Para além das fontes recrutadas pelas agências dos SIN, há que considerar outras fontes. São os *walk-ins*

[123] A comunicação pode ser efectuada recorrendo às *dead letter box* – método usado para a passagem de mensagens ou outros recorrendo a um local secreto, não necessitando por isso o recurso a meios electrónicos ou *face-to-face*

[124] *«to influence that government by feeding it false or deceptive information».*

[125] Ainda que envolva custos para treino, equipamento especial, recrutamento e criação de histórias de cobertura (Lowenthal, 2006, p. 97).

[126] O controlo de qualidade da informação é uma das principais dificuldades da HUMINT. Dependendo das suas motivações as fontes podem «fabricar» informação ou «embelezar» informação disponível através de fontes abertas ou podem trabalhar secretamente para o adversário. No que concerne aos grupos terroristas, como a penetração naquelas organizações depende das lealdades (manifestadas por laços familiares, acções, etc.) este desiderato é bastante difícil pelo que se recorre, normalmente, ao recrutamento de um membro daquele grupo.

[127] A falta de flexibilidade prende-se essencialmente com o facto de as fontes serem recrutadas tendo em conta o seu acesso à informação desejada, pelo que sempre que os requerimentos de informação alterem poderá ter de ser efectuado novo processo de recrutamento.

[128] A morosidade dos resultados é a consequência de um processo de treino de agentes (que de acordo com Lowenthal (2006, p. 95) o processo de treino de um agente pode levar até sete anos) e de recrutamento e validação de fontes algo demorado que decorre em cinco fases: (*i*) *Targeting* - Identificação de indivíduos com acesso à informação desejada; (*ii*) Acesso - obtenção da sua confiança procurando identificar vulnerabilidades e susceptibilidade do recrutado; (*iii*) Recrutamento - sugerir uma relação pessoal (com base em dinheiro, desagrado com o seu governo, chantagem, e outros); (*iv*) Gestão da fonte - fase em que o agente se reúne com as suas fontes, de forma regular para receber a informação desejada; (*v*) Termo - terminar a relação.

e as fontes diplomáticas – embaixadores, adidos, etc. Os primeiros são elementos que se voluntariam para auxiliar uma agência de *intelligence* de um Estado estrangeiro[129] que «às vezes literalmente entram na embaixada»[130] (Shulsky e Schmitt, 2002, p. 16). Como estas fontes não são sujeitas ao processo de recrutamento descrito, tornam-se inerentemente suspeitos, uma vez que o suposto «voluntarismo» pode decorrer de uma tentativa, do oponente, de passar informação falsa ou enganatória, aceder a métodos operativos ou outros, em suma infiltrar um agente no SIN em questão. As segundas, diplomáticas, são, para autores como Lowenthal, Shulsky e Schmitt, um «composto» de OSINT e HUMINT, já que os ganhos de informação são obtidos num ambiente aberto recorrendo a fontes humanas[131].

Os diplomatas podem providenciar informação acerca da situação de política interna, os adidos militares[132], podem facilitar informação relativamente ao poder militar. A informação obtida pelos canais diplomáticos tende a ser considerada como tendo menos credibilidade em função do ambiente aberto em que opera. Assim, além das percepções pessoais, há que ter a noção que qualquer decisor político ou militar sabe que, ao falar com um diplomata, aquela conversa será reportada para a capital do diplomata em questão (Lowenthal, 2006, p. 95).

Por fim, a OSINT. É um método de pesquisa que não lida, directamente, com a descoberta de segredos. No entanto, segundo Lowenthal (2006, p. 101), durante o período da guerra fria foi responsável por cerca de vinte por cento da *intelligence* acerca da URSS. Consiste na obtenção de informação com recurso a todas as fontes disponíveis[133] e cujo acesso é permitido sem qualquer medida especial de restrição (Shulsky e Schmitt, 2002, pp. 37-39). Um dos cunhos do mundo pós-guerra fria é o aumento significativo de fontes abertas, o que deixa antever que o número de sociedades fechadas e áreas negadas decresceram substancialmente, basta, tão-somente, recordar a quantidade de Estados do ex-Pacto de Varsóvia que se tornaram membros da OTAN) ou são seus «*Parceiros para a Paz*»[134]. A maior vantagem da OSINT é a acessibilidade, isto é, está facilmente disponível, ainda que requeira pesquisa.

[129] Como é o caso apresentado na obra de Christopher Andrew e Vasili Mitrokhe (2000), o Arquivo de Mitrokhe.
[130] «sometimes literally by walk into an embassy».
[131] Sem que para isso haja qualquer processo ou procedimento de recrutamento.
[132] Que têm acesso a exercícios militares e cerimónias – onde é exposto o equipamento – bases aéreas, bases navais ou outras infraestruturas civis ou militares de interesse.
[133] Os *media* – Jornais, revistas, rádio, televisão, e informação digital variada; dados públicos - Relatórios de governos, dados oficiais como orçamentos e demografia, audições, debates legislativos, conferências de imprensa e discursos; fontes profissionais e académicas - Conferências, simpósios, associações profissionais, ensaios académicos e especialistas.
[134] «*Partners for Peace* (PfP)»

Necessita de menor processamento que os métodos técnicos e humanos, não deixando de ser necessário o processamento, de todo. Outra vantagem é a capacidade de colocar a informação secreta num contexto mais vasto, acrescentando valor a essa informação. Para além do mais, para Lowenthal (2006, p. 101), torna-se de extrema importância como ponto de partida para a exploração de outros métodos[135].

Lowenthal (2006, p. 103) alerta que, contrariamente aos outros métodos, a OSINT não possui sensores, uma vez que se espera que os analistas ajam como tal. Para além do mais, ao associar o grande volume de informação inerente à OSINT, facilmente se percebe da dificuldade que representa a tarefa de separar os dados relevantes de outros, ainda que recorrendo a meios digitais e *software* especializado. De mais a mais, as OSINT não são gratuitas[136].

Ao debater a problemática das vantagens e desvantagens, Lowenthal (2006, p. 104), refere que, pela sua natureza, os diferentes métodos possuem vantagens, adequadas a determinados tipos de requisitos, mas incorporam alguns inconvenientes. Pelo que, ao projectar um conjunto alargado de métodos de pesquisa, numa determinada situação, pode-se acentuar que é possível explorar as vantagens de cada método e compensar as desvantagens de outros, pelas sinergias que criam. Para além do mais, ao ser aplicado mais que um método de pesquisa, aumenta-se a probabilidade de ir ao encontro dos requisitos estabelecidos, em virtude das sinergias que podem criar.

Num SIN, por norma, cada método de pesquisa[137] é tutelado por uma agência. Pelo que, a comunidade de *intelligence* coincide com os elementos que compõem o SIN, isto é, as agências que têm competências de pesquisa de *intelligence* incorporam os referidos SIN. Nesse sentido, em virtude da missão de cada agência, o foco não é igual o que permite a pesquisa de *intelligence* sob pontos de vista diferentes, o que vem incrementar a cooperação e a consequente integração garantindo, não só a quantidade de dados como, a, provável,

[135] A IMINT pode recorrer a imagens comerciais, pode-se fazer SIGINT na internet (recorrendo a análise de tráfego ou alterações em sítios, a MASINT, por ser relacionada com os aspectos geofísicos também pode recorrer a fontes abertas e a HUMINT através do recurso a especialistas para ampliar o conhecimento.
[136] Ainda que a internet seja gratuita, na sua maioria a fiabilidade dos dados disponíveis não representa mais que três a cinco por cento da pesquisa de OSINT, para além do mais, a aquisição de *media* impressa, bem como os sistemas informáticos que apoiam a gestão da informação são onerosos e a sua necessidade é constante.
[137] Como por exemplo, nos EUA e na Grã-Bretanha (Lowenthal, 2006).

qualidade da informação gerada na análise[138]. Contudo, porque a tutela da pesquisa de *intelligence* está dividida por entidades diferentes pode trazer constrangimentos no que concerne à partilha de informação e à cooperação entre agências, limitando a integração das mesmas, tornando as agências, por vezes competidoras[139].

1.6.2. A análise

A análise comporta actividades – como, por exemplo, o processamento e disseminação – que permitem o tratamento dos dados da pesquisa de modo a gerar conhecimento que, de acordo com Romana (2008, p. 98), se for fundamental para o problema irá incorporar o processo de decisão e, assim, garantir a diminuição da incerteza relativamente ao meio. É, por isso, uma tarefa que transcende o estar *«sentando com material recolhido, filtrando e classificando, e vir à tona com uma brilhante proposta que faz todo sentido»*[140] (Lowenthal, 2006, p. 110).

A alteração, significativa, dos «alvos» descrita anteriormente, vem dar espaço para que Treverton sublinhe que *«uma das partes crítica da agenda de transformação da informação é a análise, e a necessidade é dramática»*[141] (2009, p. 134). Aquele autor salienta que esta necessidade de reestruturação está associada ao facto dos actuais «alvos» serem «moldáveis» e adaptativos, criando uma indefinição nas distinções entre crime, terrorismo, proliferação de ADM e guerra.

Uma das formas de perceber o problema será partir do objecto de estudo da análise, os «alvos», que alteraram substancialmente as necessidades de *intelligence.*

Até ao fim da guerra fria os «alvos» tradicionais eram os Estados, enquanto que actores não-estatais ou transnacionais eram «alvos» secundários. Na actualidade a prioridade dos «alvos» alterou pelo que a forma de gerar conhecimento terá, necessariamente, de se adaptar à nova realidade, o que levanta alguns desafios.

Assim, o primeiro prende-se com a partilha de *intelligence* e o debate entre a análise competitiva e a análise cooperativa, dos elementos do sistema.

---

[138] Como atesta o relatório do congresso que investigou os atentados de 11 de Setembro.
[139] Para Thomas Hunter (2007, p. 2), a falta de cooperação entre as agências de *intelligence* é motivada por questões relacionadas com a responsabilidade territorial, o de ganho de prestígio e a disputa pela atribuição de verbas do orçamento do Estado.
[140] *«sitting down with the collected material, sifting and sorting it, and coming up with a briliant piece of propose that makes sense of it all».*
[141] *«one critical part of the agenda for reshaping intelligence is analysis, and the need is dramatic».*

Uma das principais alterações que o novo paradigma de segurança dos Estados veio ressalvar é a necessidade de partilha de *intelligence* que *«ao nível nacional ou estratégico fica difícil de alcançar»*[142] (Kiras, 2007, p. 145). James Kiras aborda esta temática nos EUA, contudo prossegue afirmando que a falta de cooperação se deve a um conjunto de factores burocráticos e organizacionais, pelo que *«são comuns para quase todos os governos democráticos com grande burocracias»*[143] (2007, p. 145). De acordo com aquele autor, numa perspectiva organizacional as agências competem entre elas para estabelecer e manter a primazia[144] dos papéis em missões específicas, de acordo com o estabelecido na lei, enquanto a regulamentação determina qual a agência que lidera e possui «comando» sobre as outras.

De certo que a competição burocrática introduz deficiências no sistema às quais não ficam imunes a eficiência e a eficácia. Estas deficiências incluem, para Kiras (2007, p. 145), perda de tempo, perda de oportunidades, bases-de-dados incompatíveis, sistemas de classificação e partilha de dados próprios e desperdício de recursos. Ocorre, por norma, em virtude de «choques de personalidades», suspeição acerca dos motivos e agendas de outras agências, o aumento de autoridade entre agências e a fricção entre agências que possuem capacidades similares ou redundantes, entre outras.

De forma a dar resposta a estes constrangimentos em várias as comunidades de *intelligence*, como a dos EUA, assume-se que o conceito de análise competitiva – possuir diferentes agências, com diferentes pontos de vista a trabalhar o mesmo problema – possui vantagens. De facto, todos os elementos do sistema possuem forças e, provavelmente, pontos de vista diferentes, no que diz respeito a diversos assuntos que, ao analisar isoladamente uma determinada situação, podem garantir uma análise mais sustentada e precisa. Contudo, para que tal seja possível é necessário, segundo Lowenthal, que todos os elementos do sistema possuam analistas suficientes, com as mesmas áreas de especialização, o que na actualidade se pode tornar incompatível com os desideratos de eficiência que os decisores assumem. Para além do mais, de acordo com aquele autor, essa redundância de meios, pode à primeira vista ser mais dispendiosa que intelectualmente produtiva tornando-se difícil de sustentar, até porque a maioria dos decisores *«não podem sobreviver tendo agências discordadas, assim*

[142] *«at the national or strategic level remains elusive».*
[143] *«are common to almost all democratic governments with large bureaucracies».*
[144] Esta primazia, de acordo com Kiras (2007, p. 145), está ligada aos recursos fiscais disponíveis para o desempenho de determinada missão.

vicia o conceito de análise competitiva»[145] (2006, p. 136).

Do outro «lado» da discussão estão os adeptos da análise cooperativa e da criação de centros de análise de *intelligence*. Esta é uma realidade que os EUA conhecem desde os anos noventa do século XX, que a comissão 9/11 recomendou após os atentados de 11 de Setembro, naquele país, de modo a incrementar a análise, *all-source*, regional ou funcional (Lowenthal, 2006, pp. 124-125). Todavia, à semelhança de outras formas de organização, a análise dos SIN não está isenta de algumas fragilidades. A primeira é que esta aproximação torna-se de alguma forma inflexível. Á semelhança de outras burocracias *«os centros não gostam de partilhar ou perder recursos»*[146] (Lowenthal, 2006, p 125) tornando a agilidade analítica mais difícil de alcançar.

Decorrente da anterior, os centros tendem a tornarem-se competidores, por recursos, com os gabinetes de análise das agências, que não pretendem ver os seus analistas fora do seu controlo e dos quais não recebem resultados directos. De mais a mais, os centros podem vir a garantir conhecimento, com base em análises técnicas, divorciando a informação do contexto político, já que é composto por peritos que tendem a ser especialistas num determinado assunto e não em contextos regionais ou nacionais. Por fim, as questões relacionadas com a tutela dos centros. Que, se estiverem co-localizados com determinada agência, as questões relacionadas com a disponibilidade dos meios é, ainda, mais notória, uma vez que existe o perigo das outras agências perderem aqueles meios durante a prestação de serviço no centro.

Não existe uma forma óptima de organizar a função análise num SIN. Cada esquema possui vantagens e inconvenientes. De acordo com Lowenthal (2006, p. 126), o objectivo deverá ser o de garantir que analistas – regionais ou especialistas – são chamados a dar o contributo se for caso disso, o que Treverton refere como a gestão matricial[147], que gera a simultaneidade da análise (2009, p. 153). Em suma, seja de forma permanente ou temporária é crucial garantir a agilidade e a flexibilidade evitando *«reter o mais delicado e relatório de saída até aos líderes tem sido possível dar o relatório aos superiores oficiais políticos, assim destacar a*

[145] *«cannot abide having agencies disagree, thus vitiating the concept of competitive analysis».*
[146] *«centers do not like to share or lose resorces».*
[147] De acordo com Chiavenato (2004: 529-531) a essência da gestão matricial é a de combinar as duas formas de departamentalização – funcional e de produto – tratando-se, por isso, de uma estrutura híbrida. "Assim, a estrutura matricial funciona como uma tabela de dupla entrada" (Chiavenato, 2004: 530). Procura tornar a estrutura funcional mais ágil e flexível às mudanças.

habilidade e a inteligência do seu povo e conquistar "pontos" com os oficiais»[148] (Hulnick, 2006, p. 963), de modo a impedir o sucedido no referente aos atentados do dia 11 de Setembro de 2001 em que a *intelligence «foi crítico a tomar decisão ao informado não foi partilhado entre agências»*[149] (Kean, 2004, p. 321). Este ponto sugere que à semelhança da pesquisa a integração e partilha de conhecimento é outro ponto fundamental.

Outro dos desafios que se coloca à função análise é a ligação aos consumidores, uma vez que a análise deve ser entendida como um processo contínuo e integrador. Fruto da fluidez do ambiente, a ligação com os consumidores assume especial importância. Primeiro, porque garante que o produto é percebido pelos que o irão utilizar, possibilitando ao consumidor a criação e teste de variadas hipóteses. Em segundo lugar, porque permite um ganho de tempo que pode ser alocado para a análise da informação. Para Treverton (2009, p. 164) a prática da análise, na actualidade, é a de que se consome muito tempo a elaborar e a coordenar documentos finais – o produto – ao invés de ter esse recurso alocado ao processo de raciocínio, gerador de conhecimento. Pelo que, ao empenhar o decisor no processo de análise poupa-se tempo que pode ser alocado ao processo de raciocínio.

No quadro da disseminação, surge, no século XXI, uma nova realidade. A necessidade de conhecer por parte de outras entidades que não os decisores políticos e militares. Treverton (2009, p. 185) sistematiza-os em oito novos tipos de utilizadores de *intelligence*: (*i*) comandantes militares tácticos; (*ii*) agências federais «domésticas»; (*iii*) Organizações Não-governamentais (ONG); (*iv*) conjunto alargado de agências federais; (*v*) autoridades locais e estaduais; (*vi*) órgãos de polícia; (*vii*) gestores privados de infraestruturas públicas; (*viii*) cidadãos privados. Sendo que as primeiras três categorias surgem no período anterior ao 11 de Setembro e à, designada, guerra global contra o terrorismo.

A primeira categoria ainda que coincida com o fim da guerra-fria, não decorre daquele conflito. De facto, o empenhamento militar no Teatro de Operações da Europa, em operações de apoio à paz, na região dos Balcãs, permitiu que os sistemas de TECHINT – SIGINT e IMINT – antes designados para compreender a URSS, fossem redireccionados para apoiar os

[148] *«to hold back the most sensitive and exiting reports until the leaders have been able to deliver the reports to senior policy officials, thus highlighting the skill and cleverness of their people and scoring «points» with the officials».*
[149] *«that was critical to informed decision making was not shared among agencies».*

comandantes militares tácticos[150]. A mesma tipologia de operações militares e outras operações de contingência facilitou o desenvolvimento de ONG, muitas vezes em áreas do globo que não haviam sido a prioridade de *intelligence* para os Estados ocidentais. No entanto, por natureza, estas organizações são cépticas relativamente aos governos e, em particular, relativamente às agências de *intelligence*. Ora, de acordo com Treverton *«eventualmente eles também receberam a ideia que alguém preocupou-se com as suas questões»*[151] (2009, p. 186)[152].

A segunda categoria é resultado do final da guerra-fria. A globalização da economia mundial, após 1989 abriu espaço para necessidades de *intelligence*, ao nível do departamento de comércio, nos EUA, e dos seus congéneres, noutros Estados. A informação económica pauta-se, essencialmente, por uma premência grande em termos de oportunidade. Traduz num enorme desafio para os SIN. Neste sentido, a pressão exercida sobre as agências de *intelligence* aumentou de forma significativa. Por um lado, mais utilizadores, por outro, menos meios. O que afecta, de forma substancial, a capacidade de conduzir análises profundas.

As restantes cinco categorias de utilizadores são produto dos atentados de 11 de Setembro de 2001. No combate ao terrorismo o esforço deve recair na prevenção, o que implica que é, para Treverton (2009, p. 186), um conflito, essencialmente, de *intelligence.* A lógica da prevenção é impedir que os terroristas possam operar. Nesse sentido, surge uma série de agências do Estado[153] que passam a estar empenhados neste conflito e necessitam de *intelligence* para se tornarem parte da solução. Ainda que as necessidades variem de agência para agência, numa perspectiva de *latu sensu* as necessidades são estratégicas e tácticas[154]. A mesma necessidade é manifestada pelas forças de polícia. Contudo, deve ter-se em consideração o espaço de jurisdição daquelas forças, de forma a adequar a *intelligence* às reais necessidades[155]. O sector privado é outra das categorias cujas necessidades surgem desde 11 de Setembro. Muitas das

[150] O apoio dos satélites, em termos de comunicações seguras, a identificação positiva de alvos, etc.
[151] *«they also eventually welcomed the idea that someone cared about their issues».*
[152] Esta ideia é sustentada no facto de que ao nível do terreno as forças militares operarem os Civil-Military Co-operation Centers (CMOC).
[153] Desde o controlo de fronteiras aos centros de controlo médico.
[154] Por exemplo, o controlo de fronteiras (que no Espaço *Shengen* é mais complexo) necessita de ter um conhecimento, estratégico, dos eixos de infiltração de grupos trans-nacionais e, no âmbito táctico, de indícios acerca de comportamentos suspeitos.
[155] Por exemplo, em Angola, províncias de fronteira terrestre como Moxico ou Cunene, têm necessariamente necessidades estratégicas e tácticas diferentes das províncias do litoral, como Luanda ou Benguela.

infraestruturas públicas são geridas pelo sector privado como, por exemplo, o sector da informação, o sector financeiro e os transportes.

A informação de que necessitam deverá ser, idealmente, talhada a cada sector em particular. Primeiro, porque prestam serviços públicos à população e no caso de pararem os constrangimentos são enormes para a sociedade[156]. Depois, são, para Treverton (2009, p. 187), símbolos da sociedade ocidental, consequentemente um objectivo para grupos terroristas[157]. Por fim, o cidadão privado que para além de necessitar de conhecer a ameaça, deve ter conhecimento de forma a identificar indícios e, acima de tudo, ter consciência de como deve reagir, caso seja necessário.

Contudo, as alterações de paradigma são difíceis de operacionalizar. A *intelligence*, produzida pelas várias agências está sujeita a protocolos de segurança, o que em larga medida dificulta a partilha entre as agências de um SIN. A este propósito Hulnik (2006) refere que o factor que afecta a confiança e uma análise integrada entre as diversas agências de um SIN é, acima de tudo, a ligação e partilha de informação entre agências. Segundo aquele autor, há uma tendência natural para que as diversas agências se centrem em demasia no paradigma da *necessidade de conhecer*. Para além do mais, se entre agências de *intelligence* de um SIN é difícil a partilha, muito mais se tornará quando se fala em consumidores que estão fora dos canais de disseminação normais dos SIN. No entanto, essa partilha pode ser o suficiente para impedir um ataque de, por exemplo, um grupo terrorista como os ocorridos nos EUA, Espanha ou Londres. Para isso há que partilhar a informação com quem tem necessidade de conhecer e, acima de tudo, em tempo, pelo que a antecipação passa necessariamente pela identificação, em tempo, do utilizador que tem necessidade de aceder a essa informação, de modo a evitar ocorrências catastróficas.

1.6.3. A Contra-inteligência

A *contra inteligência*, é a função da *intelligence* que tem como principal racional a protecção das capacidades de *intelligence* contra as actividades de *intelligence* hostis. O seu objectivo é a degradação das capacidades de pesquisa e análise de *intelligence* do adversário. Primeiro, porque nega o acesso do adversário a determinada informação, através da segurança e contra-

[156] Por exemplo, se a rede de transportes deixar de funcionar vários sectores são afectados, como, por exemplo, a economia.
[157] Veja-se, os atentados das torres gémeas, em Nova Iorque, ou do metro, em Madrid, entre outros.

espionagem. Em segundo lugar, através das operações de decepção introduz *inputs* falsos ou informação deliberadamente enganadora para que os sistemas adversários cheguem a conclusões incorrectas acerca das capacidades, intenções e acções em relação ao seu «alvo».

Das funções da *intelligence* a *contra-inteligência* (CI) é, provavelmente, de acordo com autores como Lowenthal, Shulsky e Schmittd, das mais difíceis de caracterizar. É, à semelhança da *intelligence*, simultaneamente um produto e uma actividade. Produto, na perspectiva de que é informação fidedigna acerca de sistemas hostis e outras ameaças ao Estado. Pelo que, necessita conhecer a estrutura organizacional, do adversário, o seu pessoal-chave, métodos de recrutamento e treino e detalhes de operações específicas. Como actividade, Shoulsky e Schmitt identificam as medidas passivas e activas (2002, p. 99).

As primeiras procuram negar o acesso dos sistemas hostis à informação, as segundas, procuram perceber como os SIN hostis funcionam, de forma a frustrar ou a disromper as suas actividades e, em última análise, tornar as actividades hostis numa vantagem para o próprio SIN.

Das medidas passivas fazem parte os sistemas de classificação da informação e as medidas de segurança. Os sistemas de classificação de informação têm por racional a categorização da informação de acordo com a sua sensibilidade[158]. Quanto mais sensível a informação, mais cuidado se deve ter no seu manuseamento e, consequentemente, menor o número de pessoas com o grau de credenciação[159] que lhes permite manusear tal informação. Contudo, o grau de credenciação não é suficiente para obter o acesso à informação. Nesse sentido, é estabelecido um sistema de controlo informal, o princípio da *necessidade de conhecer*[160] que permita, aos elementos que necessitam aceder à informação necessária ao cabal desempenho das suas tarefas oficiais (Shulsky e Schmitt, 2002, pp. 99-100).

[158] Neste contexto podemos associar a sensibilidade da informação ao dano que a revelação da mesma, a um poder hostil, poderá causar ao Estado. Por exemplo, o grau de «muito secreto» - danos excepcionalmente graves; «secreto» - danos sérios; «confidencial» - danos (Shulsky e Schmitt, 2002, p. 100).
[159] Grau de autorização, formal, para aceder à informação sensível (Shulsky e Schmitt, 2002, p. 100).
[160] Este sistema de controlo informal garante, para Lowenthal, a compartimentação do sistema uma vez que, apesar da credenciação um analista que trabalhe com fontes, por exemplo IMINT, pode encontrar dificuldade em aceder a informação proveniente de fontes de HUMINT (2006, pp. 148-149).

1.6.4. A acção coberta

A acção coberta (AC) tem por objectivo disromper o processo de decisão política dos decisores adversários. Independentemente da forma como se pressente, sobressai que o cerne desta actividade é a influência directa no processo de decisão política. Pelo que sendo uma das actividades de *intelligence* difere, conceptualmente, das outras funções.

Se as anteriores têm como preocupação a procura e a salvaguarda da informação, a AC procura a influência nos eventos políticos. Nesse sentido, Steiner citado por O'Brien refere que a acção coberta (AC) *«é tudo sobre fazer as coisas acontecer, enquanto inteligência consiste para tomar decisões certas sobre como para fazer acontecer»*[161] (2007, p. 25). Para além do mais, Godson citado, também, por O´Brien ao fazer a distinção entre CI e AC menciona que a CI é focada nos operacionais de *intelligence* e nos decisores políticos, enquanto a AC tem como «alvo» *«non-intelligence players»* (2007, p. 25).

É frequentemente designada de *boa opção*, seja em termos de actividade de *intelligence*, seja no contexto das RI. Ainda que usada ao longo da história da humanidade, formalizou-se e burocratizou-se, enquanto actividade de *intelligence* durante o século XX. Atingiu o ponto alto no período da guerra fria, tendo sido usada por ambos os blocos antagonistas na prossecução dos seus interesses geopolíticos (O'Brien, 2007, p. 23). No entanto a guerra fria não pôs um fim a esta actividade. De acordo com O'Brien, na actualidade, tal como durante a guerra fria, e antes, a AC *«continua a ser um instrumento usado para apoiar interesses do Estado e rivalidades ao redor do mundo»*[162] (2007, p. 24).

O âmbito da AC é bastante abrangente. Johnson e Wirtz (2004, p. 253) designam-na de *«terceira opção»*[163] – uma opção firmada entre a diplomacia e a guerra. Seguindo o mesmo racional Godson (1995, p. 156) transmite a ideia de que são as acções efectuadas por um governo para influenciar eventos, noutro Estado ou território, sem revelar o seu envolvimento. O'Brien (2007, p. 24) acrescenta que é a sua natureza coberta que permite aos Estados utilizá-la quando a primeira, a diplomacia, é insuficiente para atingir os objectivos e, a segunda, o emprego de forças armadas não é opção. Para além do mais, a natureza coberta garante a

[161] *«is all about making things happen, while intelligence consists of making the right decisions about what to make happen».*
[162] *«continues to be a tool used to support states' interests and rivalries around the world».*
[163] *third option.*

«negação plausível»[164], ou seja, que o Estado opere fora do seu território sem que a sua presença seja conhecida ou notada.

Para Johnson e Wirtz (2004, pp. 254-259), bem como para outros autores como O'Brien (2007, p. 25) as categorias de acção coberta são quatro: (*i*) propaganda; (*ii*) acção coberta política; (*iii*) acção coberta económica; (*iv*) acção paramilitar.

A primeira é, para Lowenthal (2006, p. 162), a mais antiga técnica de disseminar informação com o objectivo de um *outcome* político específico. É entendida por Janowitz *apud* (O'Brien, 2007, p. 33) como a disseminação planeada de notícias, informação, argumentos e apelos especialmente desenhados para influenciar as crenças, opiniões e acções de um grupo específico ou de um indivíduo. Focada em actividades efectuadas de forma aberta ou coberta, esta técnica é, por norma, utilizada em conjunto com outras técnicas[165]. Pode ser utilizado para o apoio de indivíduos, grupos amigáveis, exaurir o poder de adversários, criar falsos rumores de agitação política, capitalizar a escassez económica ou ataques directos a adversários[166]. O principal objectivo da propaganda é a persuasão[167].

A acção coberta política é apresentada por Lowenthal (2006, p. 162) como a forma das operações de *intelligence* intervirem mais directamente no processo político do Estado-alvo. Envolve, para Godson (1995, p. 156), o apoio e coordenação de agentes de influência e outros envolvidos nos mais altos círculos políticos, podendo, no entanto, extender-se a campos não-governamentais como sindicatos, movimentos juvenís, círculos intelectuais e movimentos religiosos, por exemplo. Tal como na categoria anterior pode ser empregue para apoiar aliados ou para impedir ameaças de concretizarem os seus objectivos[168].

---

[164] *Plausible deniability,* que segundo Lowenthal (2006, p. 166) é um conceito central à acção coberta. Procura transmitir a ideia que se o envolvimento de um Estado, em actividades de acção coberta, for conhecido o chefe de Estado pode negar o seu consentimento nessa acção. Pode, inclusivamente, afirmar, com alguma plausibilidade, que a acção foi desenvolvida pelos seus subordinados sem o seu conhecimento ou autoridade (Shulsky e Schmitt, 2002, p. 93).

[165] Por exemplo, acção coberta política.

[166] Como exemplo temos as «fugas» de informação para jornais, ou outros meios de *media* do Estado-alvo.

[167] Neste sentido O'Brien (2007, p. 33) refere que a persuasão pode ser uma mistura de ameaças e apelos que incluem um largo elemento de coacção física e psicológica. Pode incluir chantagem, subornos e ameaças de aplicação de actos de violência física como raptos e torturas, por exemplo.

[168] Utiliza vários métodos, onde os pagamentos secretos a políticos, burocratas ou a partidos políticos estrangeiros, são um exemplo e o apoio à eclosão de manifestações e interferência com as promulgações da ameaça, são outro.

A acção coberta económica é a terceira categoria. Inclui tentativas, através de meios cobertos, de disromper ou destabilizar as economias adversárias. Para o efeito, de acordo com O'Brien (2007, pp. 42-43), utiliza métodos como contrafacção de moeda estrangeira, abaixamento dos preços, nos mercados mundiais, das *commodities*[169] vitais ao adversário[170], destruição de linhas de abastecimento eléctrico, destruição de portos marítimos, entre outros. De acordo com Johnson e Wirtz em virtude da dependência económica, financeira e informática *«com hábil intercepção, a nação ou grupo de transação financeira pode ser deixada em caos, os bens do banco roubado (…) um ataque electrónico que poderia ser no mínimo como deslocar um ataque militar»*[171] (2004, p. 257).

A última, a acção paramilitar, é considerada por Johnson e Wirtz (2004, p. 257) a categoria cujo uso da violência é notório e, por isso, representa uma maior controvérsia. Godson (1995, p. 157) apresenta o apoio a grupos terroristas, movimentos insurgentes ou outro tipo de grupos não convencionais, bem como o apoio a forças governamentais que contrariem a acção destes como alguns exemplos desta actividade. O´Brien (2007, p. 43-47) acrescenta, ainda, todas as formas de assassinato[172] de indivíduos estrangeiros[173] e golpes de Estado. Para aquele autor o cerne desta categoria é a violência armada pelo que, todos os actos que sejam conduzidos num contexto de acção coberta, cuja natureza seja a violência armada, deve ser considerado como acção paramilitar.

Ao vislumbrar as categorias desta actividade fica a ideia de que é discutível considera-la uma actividade de *intelligence*, nascendo, por isso, o debate em torno desta problemática. Um dos pólos alimenta a discussão argumentando com o provável enviesamento da análise da *intelligence*, já que se está a atribuir as responsabilidades de implementação de política, de pesquisa e análise de *intelligence,* incluindo a análise dos efeitos da acção coberta, à mesma agência (Shulsky, 1995, p. 94). O outro pólo contra-argumenta que as agências de *intelligence* são as organizações que devem conduzir esta actividade. Primeiro, porque a história demonstra que se existirem organizações separadas[174] pode gerar-se falta de coordenação e

[169] Usada como referência às matérias-primas ou produtos com pequeno grau de industrialização, de qualidade quase uniforme, produzidos em grandes quantidades e por diferentes produtores (e.g. ferro, ouro, petróleo, trigo, milho, café, entre outros).
[170] Principalmente àqueles Estados que dependem da produção de uma única matéria prima.
[171] *«with skillful hacking (cyberwarfare), a nation or group's financial transactions can be left in disarray, its bank assets stolen (…) an electronic assault that could be at least as dislocating as a military attack».*
[172] Johnson e Wirtz (2004, p. 258) identificam o assassinato como outra categoria da acção coberta.
[173] Por vezes designado de *target killing.*
[174] Uma dedicada às actividades de pesquisa e segurança da *intelligence* e outra dedicada, em exclusividade, à

disputa de recursos, conduzindo a resultados catastróficos[175] (Shulsky e Schmitt, 2002, p. 95). Em segundo lugar, porque ainda que, conceptualmente, a acção coberta e a pesquisa HUMINT sejam diferentes, ambas dependem recursos similares, principalmente na cooperação secreta de agentes habilitados a operar no Estado-alvo. De acordo com Shulsky e Schmitt (2002, p. 95), na maioria dos casos os agentes que desenvolvem uma das funções podem desempenhar a outra. Para além do mais, as tarefas[176] desempenhadas para apoiar ambas as funções requerem competências, contactos e recursos similares.

Em suma, apesar do debate em torno da validade da AC enquanto actividade de *intelligence*, importa salientar que a noção de *intelligence* ficaria incompleta ao cingir, apenas, à obtenção de informação e decorrente conhecimento. Assim, se a obtenção de *intelligence* é tão importante, a sua negação também o é e uma das formas de negar a verdade ao adversário é criar decepções e induzi-lo em erro. A AC, tal como a CI garantem esse desiderato, para além de que pode, através de alguns métodos[177] paralisar a acção adversária e, assim, disromper, ainda que momentaneamente, o seu ciclo de decisão. Importa ainda, vincar, que a AC não é um substituto da política externa. É, para Godson, *«geralmente contraproducente quando usado por governo que realmente não decidiu o que quer fazer, mas quer fazer qualquer coisa»*[178] (1995, p. 167). De mais a mais, a AC é um dos instrumentos que pode ser usado quando é claro que os objectivos do Estado não podem ser atingidos, exclusivamente, por ou tão eficazmente com recurso a meios abertos, por via da diplomacia ou emprego da força armada.

acção coberta.

[175] Tendo como base a experiência americana e britânica da II guerra mundial.

[176] Assegurar as comunicações entre agentes e gestores de fontes ou pagamentos clandestinos.

[177] Por exemplo o *target killing*, subornos ou chantagem, entre outros.

[178] *«gererally counterproductive when used by a government that has not really decided what it wants to do, but wants to do something».*

1.7. A EFICÁCIA

A noção do conceito de eficácia está directamente relacionada com a concretização dos objectivos e com os resultados pretendidos. Chiavenato apresenta-nos esta noção como sendo «*uma medida do alcance de resultados, ou seja, a capacidade de atingir objetivos e alcançar resultados (...) Relaciona-se com os fins almejados*» (2004, p. 183) centra-se nos *outputs* dos processos. Assim importância desta noção, no contexto da *intelligence*, é central para se obter e manter uma capacidade credível no âmbito da redução da incerteza. O conhecimento gerado é um *input* do processo de decisão. Nesse sentido, o conhecimento pode permitir a obtenção de vantagem sobre o oponente ao garantir a rentabilização[179] dos meios do Estado, alocados à implementação da acção política, de modo a obter vantagem sobre o oponente.

Contudo, a grande dificuldade está na medição, objectiva, dos *outputs* da *intelligence*. A *intelligence* é condição suficiente[180] para que o processo de decisão se efectue. O que implica que, ainda que sem o conhecimento facultado pelas organizações de *intelligence*, o processo de decisão pode ser realizado. De acordo com Mintz e De Rouen (2010, p. 38) os decisores tendem a ver o mundo de uma forma própria[181] filtrada de forma subconsciente por crenças e experiências anteriores levando-os, por vezes, a desvirtuar a decisão. Nesse sentido, aqueles autores, apresentam *«ignorando informação crítica»*[182] (2010, p. 39), entre outras, como uma das formas de demonstrar o referido viés no processo de decisão.

Depois, o facto do resultado do processo, conduzido pelas organizações de *intelligence*, ser um intangível incrementa, de sobremaneira, os obstáculos à medição da concretização do produto final. Primeiro, a qualidade das decisões não é, necessariamente, directamente proporcional à qualidade dos *inputs*, que as organizações de *intelligence* facilitam. Depois, a qualidade da *intelligence* nem sempre é garantida, podendo em determinadas situações induzir as elites decisoras em erro, o que concorre, substancialmente, para a falta de comunicação entre decisores e OISE.

---

[179] A procura pela eficiência, que Chiavenato define como "... uma relação entre custos e benefícios, entre entradas e saídas, ou seja, a relação entre o que é conseguido e o que pode ser conseguido. Significa fazer corretamente as coisas e enfatizar os meios pelos quais elas são executadas. Relaciona-se com os meios, isto é, com os métodos utilizados" (2004, p. 183).

[180] De acordo com Freitas (1989, p. 1094) a condição é suficiente quando é requerida para "qualquer coisa exista, mas não é absolutamente necessária"; ainda de acordo com aquele autor, a condição é necessária quando é indispensável.

[181] O que se designa de factores psicológicos.

[182] *«ignoring critical information».*

1.7.1. Os atributos da eficácia

Não obstante as dificuldades inerentes à identificação de atributos mensuráveis do produto da *intelligence*, importa referir que esse desafio foi, por nós identificado, numa autora, Jennifer E. Sims. Para a Doutora Sims a eficácia da *intelligence* depende de quatro funções críticas: a pesquisa – centra-se na pesquisa de informação acerca dos competidores, incluindo a estrutura da competição, a antecipação – que tem o foco na antecipação de novas competições, a transmissão – a comunicação entre decisores e SIN e a degradação dos sistemas adversários – onde se procura a degradação das funções anteriores de forma a garantir uma vantagem competitiva.

Contudo, fruto do entendimento da *intelligence* da Doutora Sims, a sua análise não entra em linha de conta com uma das actividades da *intelligence*, a acção coberta, e a, consequente, possibilidade de disrupção do ciclo de decisão adversário. Atributo que nos parece importante, e que sem ele não é possível obter um entendimento holístico da problemática em questão.

Tendo a percepção de que a vantagem da *intelligence* se reflecte na tomada de decisão, é equacionar que a *intelligence*, sob um ponto de vista holístico, contribui, de forma directa ou indirecta, para que o decisor alcance a vantagem de decisão. Um Sistema de Informações é mais eficaz se conseguir garantir aos decisores a vantagem de decisão em relação ao adversário. Pelo que uma organização deverá direccionar todas as funções que realiza nesse sentido. Parece-nos, então, que a noção de *intelligence* apresentada pelo Prof. Heitor Romana «abre portas» para o conceito de eficácia. Através desta noção, que favorece uma abordagem holística, é possível abranger todas as funções inerentes à necessária redução da incerteza do meio, por um lado, e geradoras de incerteza no processo de decisão adversário, por outro, as duas dimensões da eficácia.

1.8. CULTURA DE SEGURANÇA

A cultura pode ser definida como o conjunto de valores, crenças, rituais, símbolos e comportamentos que partilhamos com os outros e nos ajudam a caracterizar como um grupo. Nesta linha de ideia, a cultura de segurança «é o produto de valores individuais e colectivos, atitudes, percepções, competências e padrões de comportamento que determinam o empenho e a eficácia, bem como a gestão de segurança e saúde do trabalho ao nível da empresa»

(Amaro, 2012, p. 30).

No contexto de segurança de Estado, a cultura de segurança é vista numa estreita relação com a cultura estratégica. Para tal achamos conveniente fazer uma pequena incursão sobre cultura estratégica e enfatizar a compreensão sobre a importância da cultura de segurança.

Pode dizer-se que um Estado, para ter uma política "interna ou externa" consistente, tem que possuir uma estratégia nacional. A estratégia define os objetivos dessa política e resulta da aplicação de uma força. Essa força pode ser bélica, e designa-se geralmente por *hard power*, ou pode residir em muitos outros factores e designa-se por *soft power*.

Os elementos que constituem o *soft power* nem sempre são facilmente definíveis nem totalmente compartimentáveis: podem ser culturais, podem ser tecnológicos, podem ser nichos de manobra internacional, etc.

A Estratégia pode ser definida como a «escolha do melhor caminho para se atingir um determinado objetivo com os meios (de Hard e Soft Power) disponíveis, procurando no jogo dialético minimizar sempre as vulnerabilidades, maximizar as potencialidades e neutralizar as ameaças, tendo a sua aplicação num ambiente hostil ou competitivo, ou seja, em ambiente agónico» (Garcia, 2007, p. 75).

Qualquer estratégia só é aplicável – seja ela boa ou má – depois de haver um processo de decisão. O processo de decisão depende, entre outros factores, da Informação.

Entende-se por Cultura Estratégica, «conjunto de crenças partilhadas, assunpções, e formas de comportamentos, derivados da experiência comum e das narrativas aceites (orais e escritas), que retratam a identidade colectiva e a relação com outros grupos, e que determinam os meios e os fins apropriados para alcançar os objetivos de segurança» (Johnson e Larsen, 2006).

As organizações com uma cultura de segurança positiva se caracterizam por um sistema de informações/comunicação assente na confiança mútua, nas percepções comuns acerca da importância da prevenção de riscos e na confiança da eficácia das medidas de prevenção que estão definidas a todos os níveis hierárquicos. Assim, «a cultura de segurança é a construção social aprendida e partilhada, que envolve valores, crenças e normas, relativas à segurança, transmitida por processos de interação social, e que orienta o sistema cognitivo e de acção dos

seus membros face à segurança» (Amaro, 2013, p. 30).

A segurança deve constituir parte essencial dos valores e objectivos de uma organização, não podendo ser considerado uma mera prioridade, porque as prioridades mudam. Pelo contrário, deve constituir uma valência de todas as prioridades, um desafio organizacional permanente.

CAPÍTULO II

QUADRO JURÍDICO DA ACTIVIDADE DOS ÓRGÃOS DE INTELIGÊNCIA E DE SEGURANÇA DE ESTADO

"…os Romanos fizeram aquilo que todos os príncipes sábios sabem fazer, isto é, não só fazer face às questões do presente como prevenir (…) as que podiam sobrevir no futuro, porque, antecipando a sua ocorrência, facilmente se podem remediar."

Nicolau Maquiavel[183]

[183] Maquiavel, Nicolau (2007). O Príncipe, Lisboa, Edições Sílabo. (pp. 49-50).

Neste capítulo, vamos analisar de forma concreta as disposições jurídicas referentes à actividade dos OISE, a luz da legislação em vigor, fundamentalmente sobre quatro eixos principais em torno do presente trabalho, nomeadamente: Institucionalização, definição da política de segurança nacional, funções, e os alicerces salvaguardados na legislação para a implementação da interoperabilidade.

2.1. INSTITUCIONALIZAÇÃO DOS ÓRGÃOS DE INTELIGÊNCIA E DE SEGURANÇA DO ESTADO

A actual configuração dos OISE foi estabelecida pela Lei n.º 12/02 de 16 de Agosto[184], através da qual a Assembleia Nacional cria três órgãos de inteligência e segurança do Estado, e institucionaliza o Sistema de Segurança Nacional, definindo de forma geral a missão e as atribuições dos serviços criados.

Todavia, a Lei n.º 12/02 ainda em vigor necessita ser adequação, em conformidade com a Constituição da República de Angola (CRA) de 2010, tendo em conta a designação dos três órgãos de inteligência e de segurança do Estado prescritos nas alíneas f), g) e h) do artigo 12.º, definindo: Serviço de Inteligência Externa (SIE); Serviço de Informações (SINFO); e Serviço de Inteligência Militar (SIM), estando desajustados ao actual contexto previsto no n.º 2 do artigo 211.º da CRA que estabelece «a preservação da segurança do Estado compreende componentes institucionais de órgãos de inteligência e de segurança do Estado», conjugado com os artigos 49.º, 50.º e 51.º da Secção I, do Decreto Legislativo Presidencial n.º 5/12, de 15 de Outubro[185], respectivamente institui os três órgãos «Serviço de Inteligência e de Segurança de Estado (SINSE); Serviço de Inteligência Externa (SIE); e Serviço de Inteligência e de Segurança Militar (SISM)» como Órgãos e Serviços Específicos Auxiliares do Presidente da República e Titular do Poder executivo.

[184] Lei de Segurança Nacional
[185] Aprova a organização e funcionamento dos Órgãos Auxiliares do Presidente da República.

2.2. DEFINIÇÃO DA POLÍTICA DE SEGURANÇA NACIONAL

A definição da política de segurança nacional está consagrada nos artigos 11.º, 21.º, 136.º, 202.º e 203.º da CRA, cuja execução está reservada nas competências do PR em matéria de segurança nacional[186], conjugados com os artigos 25.º e 26.º ambos do Decreto Legislativo Presidencia n.º 5/12, de 15 de Outubro.

O artigo 11.º da CRA «referente a paz e segurança nacional», no seu nº 3 estabelece o seguinte: A segurança nacional é baseada ao primado do direito e da lei, na valorização do sistema integrado de segurança e no fortalecimento da vontade nacional, visando a garantia da salvaguarda do Estado e o asseguramento da estabilidade e do desenvolvimento, contra quaisquer ameaças e riscos. Já na alínea j) do artigo 21.º, o asseguramento da paz e a segurança nacional constitui tarefa fundamental do Estado.

Compete ao Presidente da República, em matérias de segurança nacional[187]:

a) definir a política de segurança nacional e dirigir a sua execução;
b) determinar, orientar e decidir sobre a estratégia de actuação da segurança nacional;
c) aprovar o planeamento operacional do sistema de segurança nacional e decidir sobre a estratégia de emprego e de utilização das Forças Armadas Angolanas, da Polícia Nacional e demais organismos de protecção interior e dos órgãos de inteligência e de segurança de Estado;
d) convocar e presidir ao Conselho de Segurança Nacional;
e) promover a fidelidade das Forças Armadas Angolanas, da Polícia Nacional e dos órgãos de inteligência e de segurança de Estado à Constituição e às instituições democráticas.

O artigo 136.º da CRA, conjugado com artigos 25.º e 26.º do Decreto Legislativo Presidencia n.º 5/12, institui e aprova o Conselho de Seguarança Nacional como Órgão auxiliar do Presidente da República, o qual preside[188].

[186] Artigo 123.º da CRA, 2010.
[187] Competências em matérias de segurança nacional (artigo 123.º da CRA, 2010).
[188] O conselho de Segurança Nacional é o órgão de consulta do Presidente da República para os assuntos relativos à condução da Política e estratégia da segurança nacional, bem como à organização, ao funcionamento e a disciplina da Forças Armadas, da Polícia Nacional e demais organismos de garantia da ordem constitucional e dos órgãos de inteligência e de segurança de Estado em particular (CRA, artigo 136.º, n.º 1).

Os artigos 1.º e 3.º da Lei n.º 12/02 clarificam a definição e os fins de segurança nacional, no primeiro artigo, e o marco da política de segurança nacional, no terceiro artigo "a política de segurança nacional consiste no conjunto de princípios, orientações e medidas tendentes a prossecução permanente dos fins definidos no artigo 1.º da presente lei".

Os atigos 202.º e 203.º da CRA estabelecem os objectivos e fundamentos da segurança nacional, bem como o direito da República de Angola à segurança nacional e à legítima defesa.

Sendo o Presidente da República competente na definição e execução da política de segurança nacional, a sua direcção e condução estão salvaguardadas na CRA, através dos seus objectivos e fundamentos.

2.3. FUNÇÕES DOS ÓRGÃOS DE INTELIGÊNCIA E DE SEGURANÇA DO ESTADO

A função dos OISE está salvaguradada na CRA, conjugados com a Lei n.º 12/02, de 16 de Agosto e o Decreto Legislativo Presidencial n.º 05/12, de 15 de Outubro.

Os Órgãos de Inteligência e de Segurança de Estado são órgãos incumbidos de realizar a produção de informações e análises, bem como a adopção de medidas de inteligência e de segurança do Estado necessárias à preservação do Estado democrático de direito e da paz pública[189].

Os artigos 49.º, 50.º e 51.º do Decreto Legislativo Presidencial n.º 5/12 estabelece específicamente a função de cada órgão que compõe os OISE.

O Serviço de Inteligência e de Segurança de Estado é o órgão destinado a produzir informações, análises e a realização de medidas e acções de inteligência e de segurança de Estado, visando a garantia da segurança interna do país, a presevação do Estado de Direito Democrático constitucionalmente estabelecido e a protecção da população contra ameaças e vulnerabilidades[190].

[189] (CRA, artigo 212.º, n.º 1)
[190] (Artigo 49.º, n.º 1).

O Serviço de Inteligência Externa é o órgão destinado para a produção de informações, análises e para a realização de medidas e acções de inteligência e de segurança de Estado, visando a garantia da segurança externa do país, da preservação do Estado de Direito Democrático constitucionalmente estabelecido, da segurança externa e a protecção da população contra ameaças e vulnerabilidades[191].

O Serviço de Inteligência e de Segurança Militar é o órgão destinado a produzir informações, análises e a realização de medidas e acções de inteligência e de segurança de Estado, visando a garantia da segurança militar do país, da preservação do Estado de Direito democrático constitucionalmente estabelecido e a protecção da população contra ameaças e vulnerabilidades[192].

2.4. ALICERCES SALVAGUARDADOS NA LEGISLAÇÃO PARA A IMPLEMENTAÇÃO DA INTEROPERABILIDADE

Neste último eixo, procuramos demonstrar cinco alicerces fundamentais salvaguardados na legislação, que caracterizam a vontade política do Estado angolano para a implementação da interoperabilidade, sendo: a cooperação institucional entre órgãos que compõem o Conselho de Segurança Nacional; a cooperação internacional no âmbito da segurança; o factor tecnológico; a criação de bases de dados nos OISE, e a protecção da informação.

2.4.1. Cooperação entre os Õrgãos de Inteligência e de Segurança do Estado

A cooperação entre os OISE é factor preponderante para que os órgãos no exercício das suas actividade estabeleçam sinergias no interesse de segurança nacional, e a sua materialização só é funcional quando salvaguardada na legislação em vigor, pois que, dada a complexidade e carácter das informações secretas, os instrumentos jurídicos regulam o seu acesso na base da lei do segredo de Estado[193].

Em função da necessidade de cooperação na pesquisa e análise de certos fenómenos de interesse de segurança nacional, a legislação em vigor contemplou cláusulas que facilitem essa relação institucional entre os OISE.

[191] (Artigo 50.º, n.º 1).
[192] (Artigo 51.º, n.º 1).
[193] Lei n.º 10/02, de 16 de Agosto

A cooperação entre os OISE está salvaguardada na Lei n.º 12/02, de 16 de Agosto (Lei de Segurança Nacional), no artigo 9.º que estabelece o seguinte[194]:

1- Os órgãos e serviços públicos do sistema de segurança nacional exercem a sua actividade de acordo com os objectivos e finalidades da política de segurança nacional e dentro dos limites do respectivo enquadramento orgânico, o qual respeita o disposto na presente lei.
2- Sem prejuíso do disposto no número anterior, os órgãos e serviços públicos do sistema de segurança nacional cooperam entre si, designadamente, através da comunicação recíproca de dados não sujeitos a regime especial de reserva ou protecção que, não interessando apenas a prossecução dos objectivos específicos de cada serviço, sejam necessários a realização das finalidades de cada um dos outros.

Esta acção não é efectuada de forma isolada, mas sim através de uma coordenação e direcção de uma entidade, cujas atribuições foram previstas no Decreto Legislativo Presidencial n.º 5/12, de 15 de Outubro, conjugado com o Decreto Presidencial n.º 201/13, de 02 de Dezembro[195].

O artigo 1.º, no seu n.º 1 estabelece que «a Casa de Segurança do Presidente da República é o órgão com a finalidade de prestar assistência, assessoria e apoio técnico directo e imediato ao Presidente da República e Chefe de Estado no desempenho das suas funções, especialmente em assuntos de segurança nacional e na garantia de segurança e defesa presidencial[196]». O n.º 2 estabelece que «a Casa de Segurança do Presidente da República é dirigida pelo Ministro de Estado e Chefe da Casa de Segurança».

O artigo 5.º do Decreto Presidencial n.º 201/13, estabelece no n.º 2, nas suas alíneas c) e d) o seguinte:

c) Prestar assistência, assessoria e apoio técnico ao Presidente da República e Comandante-Em-Chefe nos domínios da defesa nacional, de protecção interna e de preservação da segurança do Estado;

[194] Coordenação e cooperação dos órgãos e serviços públicos de informações e ordem interna.
[195] Aprova o Estatuto Orgânico da Casa de Segurança do Presidente da república.
[196] Decreto Legislativo Presidencial n.º 5/12

d) Coordenar as relações e assegurar a ligação e a articulação institucional com os órgãos e instituições próprias de segurança nacional e com os órgãos e instituições com responsabilidades específicas na execução da segurança nacional.

2.4.2. Cooperação internacional no âmbito da segurança

A semelhança da cooperação entre os OISE, na actualidade o exercício da segurança dos Estados caminha cada vez mais para a segurança cooperativa, no sentido de fazer face às novas ameaças internacionais.

Nesta perspectiva, Angola pactua com este princípio e para o efeito salvaguardou no artigo 202.º da CRA[197], a cooperação e contribuição para a paz e seguraça internacionais, estabelecendo o seguinte:

1- Compete ao Estadado, com a participação dos cidadãos, garantir a segurança nacional, observando a Constituição e a lei, bem como os instrumentos internacionais de que Angola seja parte.
2- A segurança nacional tem por objectivo a garantia da salvaguarda da independência e soberania nacionais e da integridade territorial, do Estado democrático de direito, da liberdade e da defesa do território contra quaisquer ameaças e riscos, assim como a realização da cooperação para o desenvolvimento nacional e a contribuição para a paz e segurança internacionais.

2.4.3. Factor tecnológico

O sector das comunicações electrónicas está em constante evolução no país, de tal forma que maior parte das instituições e órgãos actualmente esteja dependente desta via de comunicação. Esta dependência tem trazido novos modelos de negócios, serviços inovadores e produtos que constituem novidade no mercado nacional.

Este quadro inovador das TIC´s sempre afectou os OISE, se termos em conta que as novas tecnologias trouxeram novas capacidades, permitindo, por exemplo, a guerra de informação em rede, com maior descentralização, onde o «*próximo da informação em tempo real*»[198]

[197] Objectivos e fundamentos da segurança nacional.
[198] «*near to real time intelligence*».

impulsiona o próprio processo de planeamento e de decisão, de forma a adequar-se à necessária flexibilidade e rapidez de resposta às novas ameaças.

Estas tecnologias necessitam de uma legislação adequada para o seu emprego, uma vez que usam, sobretudo, o ciberespaço;

Nesta perspectiva, o Estado angolano promulgou dois importantes instrumentos jurídicos, sendo um para regular as comunicações electrónicas, o Decreto Presidencial n.º 108/16, de 25 de Maio[199] e outro para proteger as redes e sistemas informáticos, a Lei n.º 7/17, de 16 de Fevereiro[200].

Os diplomas foram aprovados para acomodar essa evolução, possibilitando a intervenção do Estado, em conformidade com o plano estratégico do governo e responder, de forma eficaz e eficiente, aos novos desafios da sociedade da informação, a protecção da utilização do espaço cibernético angolano contra riscos a eles associados e promover a inclusão digital.

Para o Decreto n.º 108/16, os objectivos estãos salvaguardados nos seguintes artigos:

O artigo 4.º estabelece;

1. Os objectivos específicos de intervenção pública no Sector das Comunicações Electrónicas são os seguintes:

a) Promoção da concorrência na oferta de redes e serviços de comunicações electrónicas;
b) Defesa dos interesses económicos e sociais dos utilizadores;
c) Garantia da existência, disponibilidade e qualidade das redes e serviços de comunicações electrónicas em todo território nacional, de forma a satisfazer as necessidades de comunicação dos cidadãos e das actividades económicas e sociais;
d) Prestação do serviço universal em todo território nacional e a adequação do seu âmbito à realidade tecnológica, social e económica de Angola em cada momento;
e) Protecção da privacidade e dos dados pessoais dos utilizadores;
f) Promoção do investimento privado;
g) Garantia da disponibilidade e qualidade das ligações internacionais;

[199] Aprova o Regulamento Geral das Comunicações Electrónicas.
[200] Lei de Protecção das Redes e Sistemas Informáticos.

h) Promoção da inovação e desenvolvimento;
i) Disponibilidade, na medida do possível, de frequências e de recursos de numeração adequados para a oferta de redes e serviços de comunicações electrónicas de qualidade em todo o território;
j) Promoção do desenvolvimento do sector, assim como a utilização de novos serviços e novas redes;
k) Garantia da utilização transparente, objectiva e não discriminatória do domínio público;
l) Promoção da divulgação de informações claras, especialmente nos tarifários e nas condições de utilização dos serviços de comunicações electrónicas acessíveis ao público.

O artigo 5.º define nas suas alínea b) e g) respectivamente «*acordo de interligação*» e «*interoperabilidade*». O enquadramento destas definições na legislação, demostra a vontade política do Estado de partilha de informações em redes. A sua fundamentação está desenvolvida no capítulo seguinte da presente dissertação.

Enquanto que para a Lei n.º 7/17, o seu objecto consiste em estabelecer o regime jurídico sobre as medidades de protecção das redes e sistemas informáticos, como consta no artigo 1.º. No seu artigo 2.º, no n.º 1 estabelece que, "a presente Lei aplica-se ao ciberespaço da República de Angola, contra qualquer acto de ataque, roubo informático, ciber-ataque e incidentes informáticos".

Tendo em conta que o capítulo III retrata da *interoperabilidade,* os artigos do Decreto Presidencial n.º 108/16 e da Lei 7/17, relativos ao interesse dos órgãos de segurança, estão nele enquadrado.

2.4.4. Criação de bases de dados nos Órgãos de Inteligência e de Segurança do Estado

Como sabemos, as base de dados constituem instrumentos vitais de sobrevivência das organizações, em que o seu produto final é a transformação de dados neles conservados em informação.

É de extrema importância que, os órgãos de inteligência e segurança do Estado não descartariam de salvagurdar nas suas estruturas, a organização e regulamentação destes instrumentos que auxiliam efectivamente a sua actividade.

Assim, o exercício da salvaguarda da segurança nacional como tarefa fundamental do Estado previsto na CRA, conjugado com a Lei n.º 12/02, de 16 de Agosto, prescreve a criação de Centros de Processamento de Dados (CPD) no seu artigo 25.º, estabelecendo o seguinte:

1- Os órgãos e serviços do Sistema de Segurança Nacional, podem dispor de Centros de Processamentos de Dados, compatíveis com a nartureza dos serviços, aos quais competem processar e conservar em arquivos apropriados os dados e informações recolhidas no âmbito da sua actividade.
2- Os Centros de Processamento de Dados são criados de forma compartimentada com base na natureza específica de cada um dos órgãos e serviços do Sistema de Segurança Nacional.

O actual contexto é caracterizado pelo desenvolvimento e institucionalização das TIC para dar respota às novas exigêngias, que antes eram vistas no futuro. Estas exigências geralmente são salvaguardadas na legislação, conforme constatamos no número 1 do artigo acima referido, onde refere «*os arquivos*» sem definir os formatos destes, que tanto podem ser físicos ou lógicos, porém enfatiza o adjectivo «*apropriados*» em que as informações são processadas e conservadas, o que de certo modo salvaguarda a sua corporação no âmbito das novas tecnologias de informação e comunicação, na perspectiva da interoperabilidade.

Ademais, a Lei n.º 7/17, de 16 de Fevereiro, permite-nos ter um melhor entendimento da evolução tecnológica da república de Angola, numa perspectiva em que define "*base de dados"* no seu artigo 4.º, alínea c) como sendo *"as colectâneas de obras, dados ou outros elementos independentes, dispostos de modo sistemático ou metódico e susceptíveis de acesso individual por meios electrónicos ou outro".*

2.4.5. Protecção da informação

Na *intellingence* a informação é produto resultante da actividade dos OISE, que além da sua finalidade, é necessáriamente processada e conservada na base de dados (CPD).

A informação deve ser protegida do acesso a entes não autorizados, desde a sua recolha, processamento e exploração, análise e produção, disseminação, consumo, retorno e à conservação. Para o efeito, a sua protecção deve ser regulada com base a direitos, princípios e regras previstos no ordenamento jurídico.

No ordenamento jurídico angolano constam cinco diplomas legais fundamentais que salvaguardam a protecção da informação quanto ao seu acesso, sendo: Lei n.º 10/02, de 16 de Agosto[201], Lei n.º 11/02, de 16 de Agosto[202], Lei n.º 12/02, de 16 de Agosto[203], Lei n.º 22/11, de 17 de Junho[204] e Lei n.º 7/17, de 16 de Fevereiro[205].

A Lei n.º 10/02, de 16 de Agosto (Lei do Segredo de Estado) foi promulgada na perspectiva de evitar que os bens ou valores constitucionalmente tutelados como segurança do Estado colidam com o direito a informação, previsto no artigo 200.º da CRA[206] no n.º 2 que estabelece; «os cidadãos têm direito de ser informados pela administração sobre o andamento dos processos em que sejam direitamente interessados, bem como o de conhecer as decisões que sobre eles forem tomadas». O n.º 4 do artigo atrás referido salvagurada os fundamentos da Lei n.º 10/02, estabelecendo o seguinte: É garantido aos particulares o direito de acesso aos arquivos e registos administrativos, sem prejuízo do disposto na lei em matérias relativas à segurança e defesa, ao segredo de Estado, à investigação criminal e à intimidade das pessoas.

Na Lei n.º 10/02 destacamos os artigos 21.º, 22.º, 24.º, 25.º, 26.º, 28.º, 29.º, 32.º, 35.º e 37.º, enquadrados nos âmbitos da protecção das matérias classificadas, credenciação de segurança nacional, instruções nacionais de segurança, e de acordos de segurança.

A Lei n.º 11/02, de 16 de Agosto (Lei de Acesso aos Documentos Administrativos) foi promulgada na perspectiva de regular o acesso a documentos relativos à actividades desenvolvidas por órgãos do Estado que exerçam funções administrativas e órgãos dos institutos públicos e das associações e outras entidades no exercício de poderes de autoridade, nos termos da Lei. Este princípio está salvaguardado no n.º 2 do artigo 200.º da CRA.

[201] Lei do Segredo do Estado
[202] Lei do Acesso aos Documentos Administrativos
[203] Lei de Segurança Nacional
[204] Lei da Protecção de Dados Pessoais
[205] Lei de Protecção das Redes e Sistemas Informáticos
[206] Direitos e garantias dos administrados

Na Lei n.º 11/02 destacamos os artigos 4.º, 5.º e 7.º. Os artigos em destaque estão enquadrados nos âmbitos da definição dos documentos administrativos, interdição ao acesso de informações que possam por em risco a segurança do Estado, e do direito ao acesso[207] (que no seu n.º 7, limita por legislação própria o acesso aos documentos notariais e registrais, aos documentos de identificação civil e criminal, dados pessoais com tratamento automatizado em arquivos históricos), salvaguardado na CRA atrigo 32.º, conjugados com as Leis da Protecção de Dados Pessoais[208] e de Protecção das Redes e Sistemas Informáticos[209].

Na Lei n.º 12/02 destacamos o artigo 27.º, que establecem o seguinte[210]:

1. Os funcionários e agentes, civis ou militares, só podem ter acesso aos dados e informações conservados no Centro de Processamento de Dados desde que autorizados pelos respectivos superiores hierarquicos, sendo proibida a sua utilização com finalidades diferentes da defesa do Estado democrático de direito ou da preservação e repressão da criminalidade.
2. Os funcionários ou agentes, civil ou militar que comunicar ou fazer uso de dados e informações com violação do disposto no número anterior é punido com prisão até 3 anos, se pena mais grave não lhe for aplicável e sem prejuízo da medida disciplinar que ao caso couber.
3. Sem prejuízo dos poderes de fiscalização previsto no artigo 29.º da presente lei, nenhuma entidade estranha aos órgãos de inteligência e de Segurança do Estado e as forças e órgãos de segurança interna pode ter acesso directo aos dados e informações conservados no centro de dados.

A Lei n.º 12/02 está conjugada com a Lei n.º 7/17, que estabelece as medidads de protecção das redes e sistemas informáticos, e que actualmente constituem o núcleo da base de dados.

Na Lei n.º 22/11 vários artigos foram estabelecidos para a protecção e segurança dos dados pessoais, como os artigos 21.º alínea – a), 22.º n.º 2, alínea – a), 24.º, 26.º (n.º 3 e 5), 28.º n.º 5, alínea – a), 30.º (n.º 1, 2 e 3), 32.º, 55.º, 56.º, 57.º e 58.º. Todavia, para o caso em concreto da segurança da informação destacamos os artigos 31.º (n.º 1 e 3) e 44.º, que establecem o

[207] Artigo 7.º
[208] Lei n.º 22/11, de 17 de Junho.
[209] Lei n.º 7/17, de 16 de Fevereiro
[210] Acesso de funcionários e agentes aos dados.

seguinte:

Artigo 31º (Medidas especiais de segurança).

1. O responsável pelo tratamento dos dados deve, relativamente aos dados indicados nos artigos 13.º a 17.º e no artigo 20.º, tomar as medidas adequadas para:

a) Impedir o acesso de pessoa não autorizada aos ficheiros e às instalações utilizadas para o tratamento desses dados;

b) Impedir que os suportes de dados pessoais possam ser lidos, copiados, alterados ou retirados por pessoa não autorizada;

c) Impedir a introdução não autorizada, bem como a tomada de conhecimento, a alteração ou a eliminação não autorizadas de dados pessoais inseridos;

d) Impedir que sistemas de tratamento automatizados de dados possam ser utilizados por pessoas não autorizadas através de instalações de transmissão de dados;

e) Garantir que só as pessoas autorizadas possam ter acesso aos dados abrangidos pela autorização;

f) Garantir a verificação das entidades a quem possam ser transmitidos os dados pessoais através das instalações de transmissão de dados;

g) Garantir que possa verificar-se *a posteriori*, em prazo adequado à natureza do tratamento conforme fixado em regulamentação aplicável a cada sector, quais os dados pessoais introduzidos, quando e por quem;

h) Impedir que, na transmissão de dados pessoais, bem como no transporte do seu suporte, os dados possam ser lidos, copiados, alterados ou eliminados de forma não autorizada;

2. A Agência de Protecção de Dados pode determinar que, nos casos em que a circulação em rede dos dados pessoais referidos nos artigos 12º e 13.º a 17.º possa pôr em risco direitos, liberdades e garantias dos respectivos titulares, a transmissão seja cifrada.

Artigo 44º (Natureza e composição).

A Agência de Protecção de Dados é uma pessoa colectiva de direito público, dotada de personalidade jurídica, com autonomia administrativa, financeira e patrimonial, a quem compete, nomeadamente:

a) a fiscalização da aplicação das disposições da presente lei;

b) emitir recomendações, orientações e instruções sobre as melhores práticas no tratamento de dados pessoais;

c) emitir parecer sobre o acesso aos documentos nominativos;

d) emitir parecer sobre o sistema de classificação de documentos;

e) apreciar e decidir sobre as reclamações que lhe sejam dirigidas e garantir o exercício do direito de acesso, de rectificação, actualização e cancelamento de dados;

f) registar e publicar o registo de ficheiros de dados pessoais;

g) garantir aos titulares dos dados pessoais a obtenção de informação precisa sobre os seus direitos no âmbito do tratamento dos seus dados;

h) orientar a aplicação das medidas técnicas e de segurança necessárias e adequadas;

i) cooperar com as autoridades internacionais em matéria de protecção de dados pessoais e fiscalizar os movimentos internacionais de dados pessoais;

j) exercer a sua função sancionadora em matéria de protecção de dados pessoais, nos termos da presente lei;

k) elaborar e remeter anualmente ao titular do Poder Executivo um relatório sobre o estado de aplicação da presente lei e da sua actividade;

l) emitir parecer sobre a aplicação da presente lei e demais actos complementares.

A Agência de Protecção de Dados Pessoais é composta por sete membros, designados do seguinte modo:

a) três cidadãos designados pelo Presidente da República, dos quais nomeia o Presidente da Agência;

b) três cidadãos eleitos pela Assembleia Nacional;

c) um Magistrado Judicial eleito pelo Conselho Superior da Magistratura Judicial.

Na Lei n.º 7/17, estão enunciadas as medidas de protecção das redes e sistemas informáticos, bem como as penalizações contra qualquer acto de ataque, roubo informático, ciber-ataque e incidentes informáticos, no âmbito do ciberespaço da República de Angola. Este diploma está conjugado com a Lei n.º 22/16, na medida em que a competência da instrução dos processos de contravenção punível com multa está reservada à Agência de Protecção de Dados Pessoais, conforme consta no seu artigo 43.º, n.º 1.

O quadro jurídico da actividade dos OISE fundamentado nos quatro eixos definidos permitiu-nos avançar no capítulo seguinte, onde analisamos concretamente a interoperabilidade.

CAPÍTULO III

A INTEROPERABILIDADE

3.1. BREVE HISTORIAL

O processamento básico (ficheiros elementares, anos 1950/60) caracterizou-se por trabalhos isolados de programação; cada programa tinha os seus ficheiros. A manipulação dos dados estava reduzida às funções mais simples: ordenação, classificação, e realização de somatórios. O *osftware* pouco mais fazia do que o *input*/*output* sobre o mecanismo de armazenamento, normalmente numa banda magnética. Qualquer alteração à forma como os dados deveriam estar armazenados, implicava modificações nos programas, a sua recompilação e testes. A alteração num dado conduzia à criação dum novo ficheiro. O antigo continuava a existir e assim sucessivamente. A grande maioria dos ficheiros era utilizada numa aplicação. Havia, portanto, um alto nível de redundância, com os mesmos dados multiplicados por um número indeterminado de ficheiros.

No período dourado da utilização de aplicações de gestão de ficheiros (1960/1970), os procedimentos isolados de programação foram integrados em funções. Começaram a aparecer os primeiros casos de partilha de ficheiros entre programas diferentes. Ainda não era possível o acesso aos campos, só aos registos no seu todo. Por esta altura deram-se os primeiros passos, no sentido de isolarem as aplicações dos efeitos perversos das alterações de *hardware*. Tal como no caso anterior, também aqui os ficheiros eram de uma forma geral, desenvolvidos com um único propósito. Desenvolvia-se, por exemplo, um conjunto de {ficheiros + programas} para o processamento de salários, e outro conjunto com as características dos funcionários. Muita da informação estava repetida e era incoerente entre os ficheiros, tendo que haver vários programas com finalidades praticamente semelhantes.

No início da década de 1980 surgiram os sistemas de gestão de base de dados, que tinha a originalidade de gerirem os dados independentemente dos programas. As tabelas das bases de dados podiam ser alteradas sem que isso obrigasse a recompilação de todos os programas. A noção de modelo de dados tornou-se essencial para o desenvolvimento de bases de dados. Aos dados passaram a ser aplicados dois níveis de independência, a *lógica* e a *física*. A *independência lógica* significa que a estrutura lógica dos dados pode ser alterada sem consequências ao nível de todos os programas. Por exemplo: adicionar novos campos a uma tabela, ou criar uma nova tabela. A *independência física* verifica-se quando a organização física dos dados pode ser alterada sem que isso acarrete uma modificação global na estrutura lógica dos dados e nos programas. Por exemplo: adicionar uma nova chave a uma tabela, ou

distribuir a base de dados por dois ou mais computadores. A independência lógica é a mais difícil de atingir, dado que os programas são altamente dependentes das estruturas lógicas.

Em meados da década de 1990, foi desenvolvido de uma forma dependente, um modo de armazenar, recuperar e processar dados, pois algumas ilhas espacias dificultavam a partilha de dados, funcionalidades e poder de processamento. Foram utilizados conversores de dados; os arquivos de um determinado fabricante eram convertidos para um determinado formato, que outro fabricante pudesse ler. Esse processo surgiu da necessidade de trocar informações, dados e repassar arquivos, a partir de fabricantes diferentes.

O grande sucesso desse meio se dá pela simplicidade dos protocolos que são utizados e na capacidade da distribuição da informação através dessas redes heterogêneas. A popularidade da internet facilita a troca dessas informações e dados, e o desenvolvimento dessas técnicas na rede; serviços que são de benefício para ambos os lados (para quem envia e para quem recebe).

O que é uma base de dado? Segundo Caldeira (2011, p. 25), a expressão de base de dados está intimamente associada à noção de «uma colecção de informação». De um ponto de vista mais teórico pode-se afirmar que uma base de dados é um conjunto estruturado de informação. Uma base de dados é uma colecção de dados formalmente definida, informatizada, partilhável e sujeita a um contolo central. É ainda uma colecção de dados interrelacionados com multiplas utilizações.

Base de dados é colectâneas de obras, dados ou outros elementos independentes, dispostos de modo sistemático ou metódico e susceptíveis de acesso individual por meios electrónicos ou outros[211].

3.2. VISÃO DOS DADOS

Um SGBD[212] é uma coleção de arquivos e programas inter-relacionados que permitem o usuário o acesso para consultas e alterações desses dados. O maior benefício de um banco de dados é proporcionar ao usuário uma visão *abstrata* dos dados. Isto é, o sistema acaba por

[211] Lei n.º 7/17, de 16 de Fevereiro, lei de protecção das redes e sistemas informáticos, artigo 4.º, alínea c).
[212] Sistema Gerenciador de Banco de Dados. Para Caldeira (2011, p. 25) considera SGBDR (Sistema de gestão de bases de dados relacionais), definindo como aplicações informáticas complexas, mas essenciais em muitas áreas científicas, nomeadamente na área das ciências Sócio-económicas, onde grandes quantidades de informação necessitam de ser combinadas, ou exploradas, de diversas formas nem todas fáceis de prever.

ocultar determinados detalhes sobre a forma de armazenamento e manutenção desses dados (Siberschatz; Korth, & Sudarshan, 2010, p. 5), fazendo uma alusão conducente a uma percepção de *abstração de dados* em três níveis: físico, lógico e de visão.

Para que se possa usar um sistema, ele precisa ser eficiente na recuperação das informações. Esta eficiência está relacionada à forma pela qual foram projectadas as complexas estruturas de representação desses dados na *base de dados*[213], já que muitos usuários dos sistemas de base de dados não são peritos em computação. Os técnicos, em desenvolvimento de sistemas omitem essa complexidade desses usuários por meio dos diversos níveis de abstração, de modo a facilitar a interação dos usuários com o sistema:

a) **Nível físico.** É o mais baixo nível de abstração que descreve *como* esses dados estão de facto armazenados. No nível físico, estruturas de dados complexas de nível baixo são descritas em detalhes.
b) **Nível lógico.** Este nível médio de abstração descreve *quais* dados estão armazenados na base de dados e quais as interrelacções entre eles. Assim, a base de dados como um todo é descrito em termos de um número relativamente pequeno de estruturas simples. Embora a implementação dessas estruturas simples no nível lógico possa envolver estruturas complexas no nível físico, o usuário do nível lógico não necessariamente precisa estar familiarizado com essas complexidades. O nível lógico de abstração é utilizado pelos administradores de bases de dados que precisam decidir quais informações devem pertencer a base de dados.
c) **Nível de visão.** O mais alto nível de abstração descreve apenas parte da base de dados. A despeito das estruturas simples do nível lógico, alguma complexidade permanece devido ao tamanho da base de dados. Muitos dos usuários de base de dados não precisam conhecer todas as suas informações. Pelo contrário, os usuários normalmente utilizam apenas parte da base de dados. Assim, para que essas interações sejam simplificadas, um nível de visão é definido. O sistema pode proporcionar diversas visões da mesma base de dados.

A interrelacção entre os três níveis de abstração está ilustrado na figura 3.1.

[213] Também designado por banco de dados

Figura 3.1 – Os três níveis de abstração de dados[214]

Uma analogia com o conceito de tipos de dados em linguagens de programação pode ajudar a esclarecer a distinção entre os níveis de abstração. As linguagens de programação de mais alto nível dão suporte à noção de tipos de dados. Por exemplo, três especialistas de diferentes órgãos de inteligência (SINSE, SIE e SISM), ao acessarem a mesma base, cada um terá acesso apenas à conteúdos relacionado com o órgão a que pertence.

3.3. INTEROPERABILIDADE E GOVERNOS ELECTRÓNICOS

Segundo Castro, entende-se por interoperabilidade a capacidade de sistemas múltiplos com diferentes *hardwares* e *softwares*, plataformas, estruturas de dados e interfaces intercambiarem dados com o mínimo de perca de conteúdo e funcionalidades. Ultilizando um esquema de metadados definidos, compartilhando transferência entre protocolos[215], e *crosswalks*[216] entre esquemas, os recursos na rede podem ser buscados mais amplamente (2012, p. 20).

Interoperabilidade no âmbito das TIC pode ser definida como a capacidade de múltiplos sistemas trocarem e reutilizarem informação sem custo de adaptação, preservando o seu

[214] (Siberschatz; Korth, & Sudarshan, 2010, p. 5)
[215] O protocolo serve para acessar catálogos de outras instituições, independentemente do sistema utilizado, promove o acesso simultâneo a catálogos, compartilha registros bibliográficos e possuí interface única para fontes diferentes.
[216] Ferramenta utilizada para mapeamento entre padrões de metadados heterogênios.

significado[217].

A Interoperabilidade pode ser classificada em 3 níveis:

1. **Interoperabilidade Técnica:** capacidade de sistemas e dispositivos trocarem dados com fiabilidade e sem custos acrescidos;
2. **Interoperabilidade Semântica:** capacidade de manter o significado da informação em circulação, obtida pela utilização controlada de terminologias, taxionomias e esquemas de dados;
3. **Interoperabilidade Organizativa:** capacidade de cooperação entre organizações, obtida pela compatibilização de processos, canais, motivações e outros elementos que facilitam a obtenção de fins comuns.

Para que se conquiste a interoperabilidade, os Estados devem estar engajados num esforço contínuo para assegurar que sistemas, processos e culturas de instituições, sejam geridos e direcionados para maximizar oportunidades de troca e reuso de informações, interna e externa em benefício do Estado.

Nesta perspectiva, o Estado angolano tem direcionado as suas políticas, com a criação de diplomas reguladores do sector das TIC´s, daí ter oficializado a definição de interoperabilidade.

Interoperabilidade, «funcionalidade que permite a manutenção da comunicação e serviços de forma transparente (ou similar) entre os operadores de comunicação electrónica»[218].

A interoperabilidade serve para que um sistema aceda (com semântica[219]) à dados de outro sistema (dono) de forma simples.

Com a evolução da infra-estrutura de tecnologia de informação e comunicação, surgiu o conceito de governo eletrônico (e-gov) no qual é idealizado o acesso aos serviços e informações do governo, para todos, a toda hora e em todos os lugares.

[217] Agência para modernização administrativa (2011, p. 4).
[218] Decreto Presidencial nº 108/16, art. 5º, alínea g).
[219] A semântica é a relação entre as palavras e os pensamentos; situa-se na interface entre as palavras e a realidade, no modo como os pensamentos estão ligados a coisas e situações reais. A semântica inclui ainda um ponteiro para as emoções: para além de se referirem a coisas as palavras estão carregadas de emoções que derivam e aplicam aos mais diversos fenómenos e relações sociais (Caldeira, 2011, p. 141).

O e-gov tem a informação - especialmente no formato digital - como sua principal matéria-prima. Em todo o mundo o segmento governo é o maior produtor e consumidor de dados e informações. Para tanto, instituições governamentais investem em infra-estrutura de TIC para dar suporte a um considerável legado informacional.

A interoperabilidade envolve um campo extenso: a administração pública, os poderes do Estado, o relacionamento com a sociedade, o governo, a sociedade civil, e todo e qualquer indivíduo ou organização que utiliza-se da troca de dados e informação.

O governo eletrônico baseia-se nos padrões da interoperabilidade para a realização de projetos. A programação encontrada no governo eletrônico contém informações que fazem ligação direta com organizações, instituições e órgãos.

Segundo a revista TransInformação, (Campinas, 2008/> <GooGle), a interoperabilidade conquistou as agendas governamentais. O Governo norte-americano, britânico, canadense, australiano e neozelandês têm investido novas políticas a favor da interoperabilidade. As tecnologias de informação e comunicação são a base desse dinamismo, a partir dessa nova técnica houve muita agilidade nas empresas, não é necessária a deslocação para resolver certas pendências ou esclarecer dúvidas frequentes, o atendimento é facilitado e agil.

3.4. INTEROPERABILIDADE NA ACÇÃO DA *INTELLIGENCE*

A *intelligence* apresenta-se como um facilitador das escolhas necessárias para atingir os fins últimos do Estado.

As instituições de *intelligence* devem ser entendidas à luz da sociedade em que operam. As Informações sempre foram organizadas para fazer face a uma ou várias ameaças. Hoje elas devem ter uma organização identificada com a da ameaça principal: menos hierarquizada, em rede, extremamente flexível, com uma eficaz e eficiente coordenação do esforço de pesquisa, alterando o seu paradigma para ser mais cooperativo, multinacional e multidisciplinar (Garcia, 2008, p. 105).

Para Lowenthal os SIN, ou *intelligence community,* são constituídos, em termos de macro-estrutura, por duas áreas funcionais: a gestão e a execução. A primeira cobre os requisitos, recursos, pesquisa e produção. A segunda abrange tarefas como o desenvolvimento dos sistemas de pesquisa, pesquisa e produção de *intelligence* e a manutenção da infra-estrutura

de apoio. Contudo, aquele autor acrescenta ainda que há outra função, que não sendo das mais fortes ela terá que existir, a avaliação, cuja tarefa será de relacionar os meios – recursos: financeiros e humanos – aos fins da *intelligence* – resultados: análises e operações – o que de alguma forma poderá garantir a necessária avaliação interna que suporte a flexibilização necessária para as pressões que o meio coloca nas organizações de *intelligence* (2006, pp. 33 e 34).

Fruto dos desafios que o ambiente coloca, estruturas de *intelligence* têm de desenvolver actividades de modo a garantir que o conhecimento é gerado, tendo em vista o necessário valor-acrescentado para a tomada de decisão e é assegurada a necessária segurança, seja nos processos, fontes, necessidades ou outros. Nesse sentido, seguindo a abordagem holística a que nos propusemos, importa tratar o que Lowenthal (2003, p. 97) considera como produto das informações, a *inteligência básica*[220], por formas a aclarar o contributo da interoperabilidade na acção dos OISE.

3.4.1. *Inteligência básica*

A *inteligência básica* efectua uma compilação de dados biográficos, económicos, sociais, entre outros, apresentando os seus produtos na forma de monografias, estudos de caso, ordem de batalha, mapas entre outros (Hedley, 2009, p. 214).

Tenta descrever a visualização de uma imagem fictícia, tão próxima quanto possível de uma real, com a criação de um cenário, logo no início do tratamento da informação respeitante aos factos inalterados[221]. Neste tipo de produto, podemos encontrar os produtos de análise de tendências em que se tem uma forte relação com o planeamento de cenários (Amaral, 2008, p. 266) que são mantidas em base de dados. Mantêm-se continuamente actualizadas e são essencialmente descritivas.

3.4.2. Interoperabilidade na *intelligence*

Sendo a interoperabilidade, a funcionalidade que permite a manutenção da comunicação e serviços de forma transparente (ou similar) entre os operadores de comunicação electrónica, definimos a interoperabilidade na *intelligence* em três perspectivas na visão do *acordo de*

[220] *basic intelligence*.
[221] Como exemplo, no âmbito militar se tem a descrição da ordem de batalha de uma força.

interligação[222] «1- interligação entre os sistemas dos Órgãos de Inteligência e de Segurança do Estado ou conexão inter-órgãos na estrutura do Estado; 2- interligação dos sistemas dos Órgãos de Inteligência e de Segurança do Estado com os sistemas de Serviços congéneres, de organizações internacionais e regionais e; 3- interligação do sistema da base de dados nacional ao sistema dos Órgãos de Inteligência e de Segurança do Estado», com finalidade de contribuir na acção dos Órgãos de Inteligência e de Segurança do Estado:

3.4.2.1. Interligação entre os sistemas dos Órgãos de Inteligência e de Segurança do Estado

Permite a partilha de *intelligence*, possibilitando a consumação do paradigma da *necessidade de partilha*, tornando os órgãos mais ágeis e com capacidades de adaptação constante ao meio, isto é, mais flexiveis, partilhando informações de interesse comum; neste particular a interoperabilidade desburocratiza as sinergias entre os OISE na sua actividade.

A complexidade da actual ameaça implica a existência de ferramentas de apoio à condução política, evitando a surpresa estratégica, tendo como prioridade máxima a detecção da ameaça.

Este sistema só é viável se a actuação dos serviços de informações forem céleres, através de um processo de informações dinâmico e ágil, sendo continuamente alimentado por indicadores e por informações já processadas, havendo a necessidade de ágeis canais de comunicação entre o *desk analysis*[223] e os operacionais (Romana, 2005, p. 77).

3.4.2.2. Interligação dos sistemas dos Órgãos de Inteligência e de Segurança do Estado com os sistemas de Serviços congéneres, de organizações internacionais e regionais.

Permite a consumação e o reforço da segurança cooperativa entre os Estados, Organizações Internacionais e Regionais. Esta cooperação estará assente nas convenções internacionais de que Angola seja parte, bem como nos acordos de cooperação no domínio de inteligência e segurança assinados com outros Estados parceiros.

[222] Definido como «acordo celebrado entre dois ou mais operadores de comunicações electrónicas cujo objecto é garantir a interoperabilidade das respectivas redes» [Decreto Presidencial nº 108/16, art. 5º, alínea b)].
[223] *Analista de produção.*

Muitos dos produtos de informações são efectuados por um só analista. Podendo também, receber contributos de outros analistas ou mesmo de serviços de informações congéneres (Lowenthal, 2003, p. 97).

O incremento destes sistemas nos OISE é de elevada relevância para os decisores. Os analistas têm que reagir duma forma mais célere, face aos diversos eventos, que são variáveis na unidade temporal.

3.4.2.3. Interligação do sistema da base de dados nacional ao sistema dos Órgãos de Inteligência e de Segurança do Estado

Permite a efectivação da *inteligência básica* no processo de análise e produção de informação. A *inteligência básica* responde às necessidades gerais e permanentes de uma organização, pelo que é produzida pela obtenção e análise de dados similares e constantes, de modo rotineiro e programado. A existência de uma reserva adequada é uma condição essencial para o êxito da *estimate intelligence*[224] (Esteban, 2007, p. 209).

Este produto de informações está relacionado com necessidades pontuais, onde são criados os cenários próximos da realidade, para permitir a continuação do tratamento. Toma especial feição no tratamento de material multiforme (Rodrigues, 2009).

Os técnicos de informações actuam com base em procedimentos regulares, formas de actuação e comportamentos, que providenciam uma determinada linha de conduta que permite avaliar uma linha de acção.

Procuram-se acções que estejam fora da normalização de procedimentos de um determinado actor, onde são identificados os indicadores, definidos como manifestações, positivas ou negativas, de uma determinada conduta, previamente seleccionada, identificando aspectos relacionados com os preparativos para uma possível agressão (Davis, 2009, p. 173).

As operações humanas e técnicas desencadeiam uma estreita actividade operacional, na tentativa de despoletar a informação a respeito da ameaça, avaliando o seu comportamento,

[224] O melhor resultado do trabalho dos analistas de informações é apresentado de forma a que se permita projectar o futuro. Esses resultados são geralmente conhecidos como *estimate intelligence* [informações]. Esta designação é universal e transversal às diferentes comunidades de informações, com excepção dos serviços de informações ingleses que o definem como *assessment* (Johnson, 2009, p. 2)

validando ou negando a conduta da mesma, como potencial ameaça, de acordo com a sua actuação (Baud, 2002, p. 251).

Para o efeito, concebemos um diagrama [figura 3.2], onde as três perspectivas são ilustradas, e prestamos atenção aos níveis de acesso às informações nos sistemas de base de dados, tendo como pivô os dois últimos, dos três níveis de abstração de dados, que permitiu-nos defini-los em dois níveis: Nível 1 e Nivel 2.

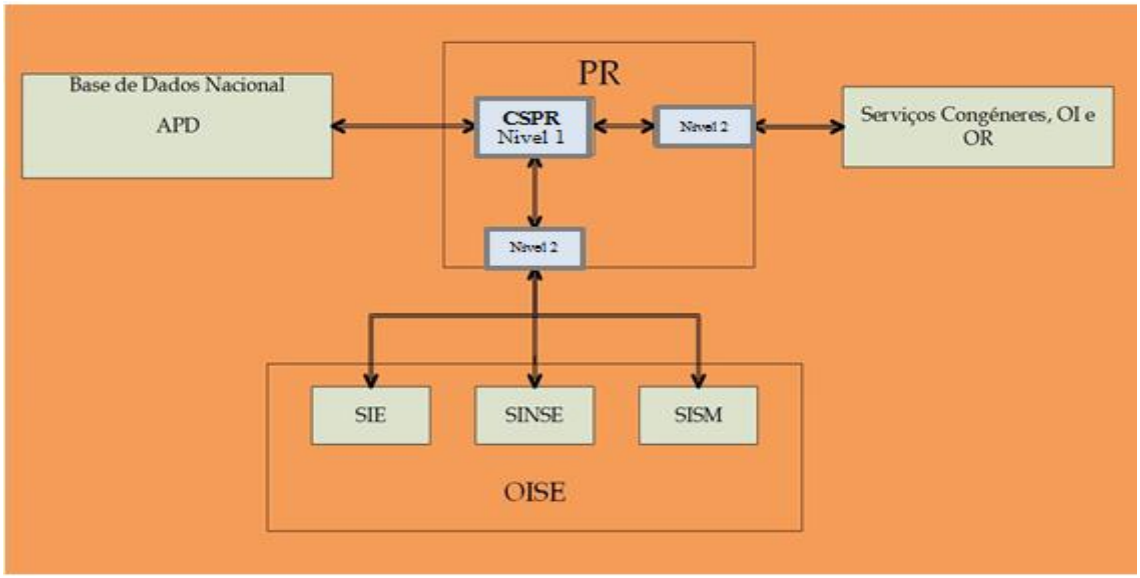


Figura 3.2 – Interoperabilidade na intelligence[225]

Nível 1: Este nível satisfaz a terceira perespectiva [interligação dos sistemas da base de dados nacional ao sistema dos OISE]. No diagrama é demonstrado que na efectivação da *basic intelligence* os OISE (SINSE, SIE e SISM) têm necessidade de acessar a base de dados nacional e de intercepção de dados. Tendo em conta que a lei prevê a protecção de dados pessoais e por via disso foi instituída a Agência de Protecção de Dados (APD), há limitições dos OISE acessarem a base de dados nacional de forma directa, sem autorização e controlo de uma entidade vocacionada. Por outro lado, a Lei n.º 22/11, de 17 de Junho, conjugado com o Decreto Presidencial nº 108/16 de 25 de Maio, no seu artigo 75º[226] alínea f, estabele o seguinte; «dispor de interfaces para conexão com os órgãos judiciários, de segurança e ordem pública». O que de certo modo salvaguarda a interligação do sistema da base de dados nacional aos OISE.

[225] Concebido pelo autor.
[226] Obrigações de interligação

Na mesma perspectiva, a Lei n.º 7/17, de 16 de Fevereiro, no seu artigo 39.º estabelece que "os operadores de comunicações electrónicas acessíveis ao público devem assegurar aos órgãos de inteligência e de segurança do Estado mediante autorização prévia do Magistrado competente, para proceder a intercepção de comunicações, nos termos do artigo 212.º da Constituição da República de Angola", caso contrário, compete à Agência de Protecção de Dados Pessoais a instrução dos processos de contravenção, conforme está plasmado no artigo 43.º da mesma lei.

Sendo a Casa de Segurança do Presidente da República (CSPR), o órgão com a finalidade de prestar assistência, assessoria e apoio técnico directo e imediato ao Presidente da República e Chefe de Estado no desempenho das suas funções, especialmente em assuntos de segurança nacional e na garantia de segurança e defesa presidencial[227], o seu dirigente[228] constitui a entidade vocacionada para o controlo do acesso à base de dados nacional pelos OISE.

Para o efeito, através de códigos de acesso[229] a CSPR regula este acesso no nível 1, para evitar transgressões aos intervenientes.

É importante aclarar que no interesse de segurança nacional, o acesso à base de dados nacional tem procedimentos previstos nas Leis n.º 10/02, 11/02, 12/02, 22/11 e 7/17, Decretos Presidenciais n.º 201/13 e 108/16. Todavia, como a actividade dos OISE são dirigidas pelo PR como Comandante-Em-Chefe, competente na definição da política de segurança nacional e dirigir suas acções[230], associada a existência na estrutura orgânica da CSPR o Centro de Direcção, Telecomunicações e Informática[231], constitui o centro pelo qual a base de dados nacional é interligada.

De acordo com o artigo 27.º do decreto Presidencial 201/13, o Centro de Direcção, Telecomunicações e Informática, dentre várias atribuições, no seu n.º 2, alíneas a) e b) estabelecem o seguinte[232]:

[227] Decreto Legislativo Presidencial nº 5/12, de 15 de Outubro, art. 15º.
[228] O Ministro de Estado e Chefe da Casa de Segurança do PR.
[229] Dado ou senha que permite aceder, no todo ou parte e sob forma inteligível, a um sistema de informação (Lei n.º 7/17, de 16 de Fevereiro, artigo 4.º, alínea i).
[230] CRA, 2010, art. 123º
[231] Arigo 27.º do Decreto Presidencial n.º 201/13.
[232] Ao Centro de Direcção, Telecomunicações e Informática do Presidente da República e Comandante-Em-Chefe compete o seguinte:

a) Assegurar as telecomunicações e tecnologias de informação de direcção do Presidente da República e Comandante-Em-Chefe;
b) Assegurar o Centro de Dados da Casa de Segurança do Presidente da República.

Com base a *visão de dados* no «nível de visão» fundamentada no *subcapítulo 3.2*, os usuários (OISE) da Base de Dados Nacional por intermédio do Centro de Dados da CSPR não precisam conhecer todas as suas informações, normalmente utilizam apenas parte da base de dados de acordo as informações de interesse de cada Órgão. O sistema pode proporcionar diversas visões da Base de Dados Nacional aos OISE em tempo real, sob supervisão e controlo do Centro de Dados Casa Segurança do Presidente da República.

Nível 2: Este nível satisfaz a primeira e a seguanda perespectivas [interligação entre os sistemas dos OISE ou conexão inter-órgãos na estrutura do Estado; e interligação dos sistemas dos OISE com os sistemas de Serviços congéneres, de organizações internacionais e regionais]. No diagrama é demonstrado que a interligação entre os sistemas dos OISE e entre os sistemas de serviços congéneres seja regulada e controlada través do Centro de Dados da CSPR que corresponde o nível 1.

Com base a *visão de dados* no «nível lógico», o Centro de Dados da CSPR é o órgão com reserva de administrar as bases de dados como um todo e decidir quais informações devem pertencer no nível 2, tanto na interoperabilidade entres os sistemas dos OISE, como na interoperabilidade entre os sistemas dos OISE e dos serviços congéneres.

O Centro de Dados da CSPR jogará um papel preponderante, na medida em que funcionará como um sistema de gestão de relações inter-bases de dados para ambos os níveis, de modo que todos os dados e informações inseridos através dos sistemas internos[233] ou externos[234] sejam tratados no sistema central do nível 1, e este dicidir na base das seguintes funções:

a) **Resposta rápida aos pedidos de informação.** Como os dados estão integrados numa única estrutura (Centro de Dados da CSPR), a resposta a questões complexas processa-se com mais rapidez.
b) **Acesso múltiplo.** O *software* de gestão do Centro de Dados permite que os dados sejam acedidos de diversas maneiras. Nomeadamente, os dados podem ser

[233] Que correspondem aos OISE
[234] Que correspondem aos serviços congéneres

visualizados através de pesquisa sobre qualquer um dos campos da tabela[235].

c) **Flexibilidade.** Em consequência da independência entre dados e programas, qualquer alteração num desses elementos não implica modificações drásticas no outro.
d) **Integridade da informação.** Dada a absoluta exigência de não permitir a redundância, as modificações de dados são feitas num só sítio, evitando-se assim possíveis conflitos entre diferentes versões da mesma informação.
e) **Melhor gestão da informação.** Em consequência da localização central dos dados, sabe-se sempre «como» e «onde» está a informação, assim como «quem» a solicita.

Após uma análise das funções da interoperabilidade na inteligência, há necessidade de uma reflexão sobre a segurança dos sistemas, como suporte principal da sua implementação.

3.5. A CIBERSEGURANÇA E O CONTRIBUTO À INTEROPERABILIDADE

Como atrás nos referimos, o governo eletrônico baseia-se nos padrões da interoperabilidade para a realização de projetos. A programação encontrada no governo eletrônico contém informações que fazem ligação direta com organizações, instituições e órgãos.

O advento da Internet como infra-estrutura global de comunicações de baixo custo e a banalização do computador pessoal permitiram a criação de serviços em linha e o rápido crescimento da informação digital circulante ou armazenada, alterando, de forma substancial, o paradigma da segurança informática (Santos, 2013, p. 226).

Àquele autor continua fazendo alusão de que esta transformação veio criar oportunidades para actores existentes e facilitar o surgimento de novos actores do crime, alargando, assim, o espectro de ameaças e dicipando as fronteiras ou os domínios de segurança existentes. A oportunidade que o ciberespaço proporciona aos criminosos levou a que crimes comuns praticados no mundo real fossem mimetizados no mundo virtual, tirando partido do relativo grau de anonimato e da velocidade com que as suas operações podem ser realizadas, mas também da inadequação da legislação e da incapacidade das forças e serviços de segurança para lidar com este problema novo. Desde a forma como interagimos com o Estado ou com o sector bancário, até a forma como desenvolvemos as nossas guerras (*information warfare*), o palco das actividades tem-se recentrado no plano virtual que designamos de ciberespaço, em

[235] Uma tabela relacional, ou simplesmente tabela, é a estrutura elementar de armazenamento numa base de dados (Caldeira 2011, p. 84)

detrimento do plano físico.

É a combinação entre a quantidade de informação ligada em rede e a crescente complexidade dos sistemas computacionais e a aplicações de suporte para os mais variados fins, que torna estes sistemas e a informação neles contida em alvos extremamente vulneráveis a ataques. Há algum tempo que estrategas e especialistas da área de segurança das redes e da informação vêm a alertar as autoridades para possíveis vulnerabilidades resultantes do rápido crescimento da Internet e da maior dependência das sociedades nesta infra-estrutura (Libicki, 1995; Denning, 2000; Arquilla, 2001).

A protecção do ciberespaço acarreta novos e grandes desafios e muito há por fazer, quer no plano nacional, quer internacional. Com diferentes níveis de responsabilidade, tanto a indústria, como os cidadãos, como o Estado são partes interessadas na cibersegurança como garante dos bens jurídicos fundamentais. Muito tem vindo a ser feito a nível nacional e internacional em prol desta garantia. No caso de Angola, há uma estratégia nacional para garantir a segurança do seu ciberespaço, e por via disso, foi aprovada a Lei n.º 7/17, de 16 de Fevereiro, que estabelece o regime jurídico sobre as medidas de protecção das redes e sistemas informáticos.

Por tudo isto, importa analisar a segurança do ciberespaço de uma forma holística e elevar a percepção das entidades, sobretudo, do Estado, para a necessidade de acompanhar o desenvolvimento tecnológico com políticas e medidas de combate às novas ameaças que o mundo virtual apresenta. Razão pela qual envolvemos a temática da Cibersegurança a partir de uma perspectiva nacional e reflectir o seu contributo à interoperabilidade, na medida em que a sua aplicação incide fundamentalmente na exploração da base de dados através dos sistemas informáticos.

Assim sendo, achamos conveniente primeiro discernir o espectro de ameaças que pairam no ciberespaço. "O conjunto das actividades que podem tirar proveito, de uma ou outra, da forte dependência dos Estados e das empresas relactivamente ao uso das TIC, afectando negativamente o seu funcionamento, pode ser dividido em várias categorias de acordo com as motivações e o perfil dos seus autores, a saber: cibercrime, desobediência civil electrónica e hacktivismo, ciberterrorismo e ciberguerra" (Santos, 2013, p. 234), ou qualquer acção natural ou humana que possa causar danos à integridade, à disponibilidade ou à confidencialidade de

um sistema, qualquer que ele seja (Gomes, 2013, p. 160).

Cibercrime – o crime cometido com o recurso aos sistemas electrónicos e as novas tecnologias de informação e comunicação[236].

Todo acto em que o computador serve de meio para atingir um objectivo criminoso ou em que o computador é o alvo desse acto (Martins, 2003; Brenner and Schwerha, 2004, pp. 111-114).

Hacktivismos ou desobediência civil electrónica – "a convergência entre o activismo social e o *hacking",* tirando partido da cobertura mediática usualmente garantida a este tipo de evento como forma de promoção de uma causa política (Denning, 2001, p. 239).

Ciberterrorismo – ataque ou tentativa de ataque à rede de comunicação, computadores e informação neles contida, com o objectivo de intimidar ou coagir um governo ou o seu pessoal para atingir fins políticos ou sociais. Para ser considerado ciberterrorismo, o ataque deve resultar em violência contra pessoas ou propriedade, ou pelo menos causar dano suficiente para provocar medo (Denning, 2000).

Ciberguerra – conjunto de acções com vista a obter superioridade de informação para a estratégia nacional militar afectando a informação do adversário e dos seus sistemas ao mesmo tempo que defendemos os nossos (Denning, 2000). No plano militar, a ciberguerra concentra as capacidades de defesa das redes, dos sistemas e da informação de caracter militar e as capacidades ofensivas de espionagem militar e de retaliação a ataques (Santos, 2013, p. 247).

Vários factores têm contribuído para destacar na agenda política dos Estados a protecção do ciberespaço. Por um lado assistimos a um desenvolvimento acelerado da sociedade da informação e a uma crescente dependência das TIC em funções vitais do funcionamento dos países. Por outro, este "mundo em rede" desenvolveu um novo plano de condução de conflitos com características únicas, que obriga a uma redefinição das políticas de segurança e de defesa nacionais.

Não existe uma definição globalmente aceite para cibersegurança[237]. Esta varia consoante o

[236] Lei n.º 7/16, de 16 de Fevereiro, artigo 4.º alínea g).
[237] Existem diferentes tipos de entidade a trabalhar o tema, com perspectivas muito diferentes. Esta situação leva a que o conceito de Cibersegurança seja usado para designar coisas muito diversas como, por exemplo,

tipo de organismo que a define e o modelo de referência onde este se enquadra (Santos, 2013, p. 252).

Não sendo totalmente disjuntos, estes modelos apresetam diferenças relevantes nos respectivos objectivos, nos seus principais actores, nos meios técnicos disponíveis e no enquadramento jurídico aplicável. No modelo de guerra os ciberataques são vistos como actos de guerra, pelo que a resposta tem como centro de gravidade a acção militar, com todos os recursos disponíveis, apenas sujeita na acção pelo Direito Internacional dos Conflitos Armados[238] e pelo Direito Internacional dos Direitos Humanos. No modelo de perseguição criminal/judicial os ciberataques são vistos e definidos como actos criminalmente relevantes, passíveis de sancionamento dentro do edifício jurídico do respectivo país. Já para o modelo de protecção simples contribui um vasto espectro de autores com o objectivo último de proteger os activos das organizações e dos indivíduos. Esta protecção compreende todos os meios tecnológicos permitidos na lei, bem como as normas técnicas e os instrumentos legais, e é realizada, em primeira instância, pelos donos desses activos, mas também pelo Estado, através das suas forças e serviços de segurança e autoridades reguladoras, ou mesmo empresas privadas em regime de *outsourcing* e fabricantes de *hardware* e de *software* especializados.

information assurance, business continuity ou protecção de infra-estruturas críticas da informação.

[238] O Direito Internacional dos Conflitos armados é composto pela Convenção de Genebra de 1948 e Protocolos Adicionais. Estas sujeitam a acção militar a um conjunto de princípios que visam evitar o uso indiscriminado da força, nomeadamente os princípios da proporcionalidade dos meios e o da distinção entre o plano civil e o militar.

CONCLUSÕES

A nossa pesquisa, como devidamente referenciada na parte introdutória, conduziu-nos a fontes diversas e, por conseguinte, a uma multiplicidade de informações cuja qualidade e pertinência, o tempo e a necessidade de cumprir prazos foram o "calcanhar de Aquiles" para a sua abordagem mais ampla do que a que trouxemos nos capítulos anteriores. Não obstante, a vontade e a responsabilidade a nós recaída, foram também factores que, à laia de catalisadores, transformaram os momentos difícieis e de franca inspiração em valor acrescentado, colocando-nos sempre diante do nobre desafio de apresentar um trabalho qualitativamente à altura do nível académico que se busca com esta dissertação.

Lembramos que para abordar a temática proposta "Interoperabilidade: contributos para a eficácia do produto da acção dos Órgãos de Inteligência e de Segurança de Estado" definiu-se como fio condutor a seguinte questão central *Como compreender a importância da interoperabilidade entre os órgãos de segurança do Estado?* Esta questão e outras que se impuseram foram linearmente respondidas, sem, no entanto, exgota-las, por não ser este o nosso objectivo e por acharmos ser este um campo muito vasto, aliás se atendermos também a nossa condição de propedêuticos no que toca a pesquisa científica.

Inicialmente, preocupamo-nos em encontrar a compreensão do conceito *intelligence,* bem como o entendimento dos sistemas de inteligência e de segurança de Estado. Foi possível identificar, que a *intelligence* é uma actividade desempenhada por Estados, de forma a facilitar a consecução dos seus fins últimos e que os sistemas de inteligência e de segurança de Estado são organizações permanentes designadas para apoiar esse desiderato, no quadro da salvaguarda do Estado contra ameaças e riscos à sua segurança. Para além do mais, relativamente à organização das suas estruturas, percebemos que reflecte as necessidades e prioridades do governo quanto à *intelligence,* enquanto preservação da segurança do Estado.

É nesta ordem de ideias que aferimos ainda que a *intelligence* é um campo de estudo que privilegia a convergência de diferentes áreas das ciências sociais, dada a natureza pluridimensional dos riscos e objectivos a salvaguardar, onde somente o estudo a esta dimensão permite dar resposta capaz às necessidades do processo de decisão.

De seguida, e com o enfoque colocado na legislação, entendemos que o enquadramento das disposições jurídicas referentes à actividade dos Órgãos de Inteligência e de Segurança do

Estado de Angola, à luz da legislação em vigor, está preservado nos âmbitos da institucionalização, da definição da política de segurança nacional e das suas funções. Ademais, demonstramos os alicerces salvaguardados na legislação para a implementação da interoperabilidade, procurando, a partir da interoperabilidade na *intelligence*, perceber que a sua função na acção dos OISE permite a partilha de intelligence, o reforço da segurança cooperativa e a efectivação da *inteligência básica* no processo de pesquisa, análise e produção de informação.

As hipóteses formuladas inicialmente mereceram especial dedicação, e esta, resultou na confirmação do que a priori fora levantado, o que, concomitantemente, foram passíveis de validar as diversas hipóteses e de responder às questões derivadas. Por via disso, foi encontrada uma resposta à questão central através da delineação e apresentação da importância e do contributo da interoperabilidade na eficácia do produto da acção dos Órgãos de Inteligência e de Segurança do Estado, tal como deixamos sinteticamente demostrado abaixo:

Relativamente a primeira hipótese, por exemplo, aferimos que, com base na definição do IDN relativa à segurança nacional, é vista como a situação que garante a unidade, a soberania e a independência da Nação, a integridade e a segurança das pessoas e dos bens; o bem-estar e a prosperidade da Nação; a unidade do Estado e o desenvolvimento normal das suas tarefas; a liberdade de acção política dos órgãos de soberania e o regular funcionamento das instituições democráticas, no quadro constitucional, a sua preservação é garantida pela *intelligence*.

Assim, a visão holística do conceito de *intelligence* é entendida em três perspectivas, a organização, o processo e o produto, perspectivas estas que o conceito de *intelligence* utiliza-nas sob dois prismas, sendo o primeiro, uma noção em sentido lato, assume-se que a *intelligence* é toda a informação pesquisada, organizada ou analisada de forma a satisfazer as necessidades de qualquer decisor, desde que envolto numa empresa de competitividade; o segundo prisma, em sentido restrito, a *intelligence* deve ser entendida como a pesquisa de informações sem o consentimento, a cooperação ou o conhecimento dos «alvos», de forma a alimentar as necessidades do Estado, tendo, por isso, o segredo um papel fulcral.

A segunda hipótese, começa a ganhar sustentação com a tese segundo a qual a creditação da estrutura determina o sucesso da actividade das informações dessa organização (Hannah, O'

Brien, & Rathmell, 2005, p. 4). Sendo a República de Angola um Estado democrático de direito, o exercício das suas instituições deve ser em obediência à constituição e às demais leis vigentes. Por exemplo, o Presidente da República é um órgão de soberania, o qual é auxiliado por instituições públicas no exercício das suas funções. Dentre vários órgãos, se destacam os OISE que constituem órgãos e serviços específicos auxiliares do PR e titular do poder executivo, vocacionados à preservação da segurança do Estado. Por conseguinte, a sua acção goza de legitimidade quando salvaguardada na CRA e nas demais leis vigentes.

Em suma, a segurança nacional é baseada no primado do direito e da lei, na valorização do sistema integrado de segurança e no fortalecimento da vontade nacional, visando a garantia da salvaguarda do Estado e o asseguramento da estabilidade e do desenvolvimento, contra quaisquer ameaças e riscos[239].

Em resposta a terceira hipótese, deprrendemos que a criação de novas técnicas de recolha de dados, interligação e cruzamento de informação entre órgão, através da materialização de uma base de dados que seja guarnecida por operacionais, que simultaneamente efectuam a gestão de fontes, com a garantia de se produzir um conhecimento crítico sobre cenários criados ou previamente definidos numa perspectiva de ganho de tempo, exige a criação de novos conceitos de análise. É nesta ordem de ideia que os Órgãos de Inteligência e de Segurança de Estado aparecem com o fim último de alimentar o processo de decisão, produzindo e analisando informação e identificar correctamente o problema posto ao decisor, cujas "deliberações" são tipicamente caracterizadas pelo risco substancial, pela grande incerteza e pelo valor do que está em jogo para o Estado.

Na actualidade os OISE estão preocupados a ajustar os seus serviços à dinâmica das novas ameaças, adaptando-os à era da informação e do conhecimento, procurando permanentemente evitar a burocracia, que em muitos casos está caracterizado por um planeamento normalizado e operações cíclicas onde não escapa a rotina. Daí que é necessário incrementar o contacto entre oficias de *intelligence*, as suas fontes e a produção de informações, integrando uma rede de flexibilização de informações através de análise cuidada. Os *analistas de produção* continuam a insistir na análise de produtos ao invés de efectuarem somente um refinamento do produto do analista operacional. Esta insistência, geralmente, ocorre pelo facto de não se aplicar a interoperabilidade durante o processo de pesquisa e, análise e produção das

[239] Artigo 11.º da CRA.

informações, por forma a garantir fiabilidade na consolidação do produto da *intelligence*, o que de certo modo coloca em dúvida a sua eficácia.

A interoperabilidade na *intelligence* definímo-la em três perspectivas: «1- interligação entre os sistemas dos Órgãos de Inteligência e de Segurança do Estado ou conexão inter-órgãos na estrutura do Estado; 2- interligação dos sistemas dos Órgãos de Inteligência e de Segurança do Estado com os sistemas de Serviços congéneres, de organizações internacionais e regionais e; 3- interligação do sistema da base de dados nacional ao sistema dos Órgãos de Inteligência e de Segurança do Estado», com finalidade de contribuir na acção dos Órgãos de Inteligência e de Segurança do Estado, contribuindo significativamente para:

1- A partilha de *intelligence*, com vista a consumação do paradigma da *necessidade de partilha*, tornando os órgãos mais ágeis e com capacidades de adaptação constante ao meio, isto é, mais flexíveis, partilhando informações de interesse comum; neste particular a interoperabilidade desburocratiza as sinergias entre os OISE na sua actividade.

2- O reforço da segurança cooperativa entre os Estados, organizações internacionais e regionais. Esta cooperação estará assente nas convenções internacionais de Angola seja parte, bem como nos acordos de cooperação no domínio de inteligência e segurança assinados com outros Estados parceiros.

3- A efectivação da *inteligência básica* no processo de pesquisa, análise e produção de informação. A *inteligência básica* responde às necessidades gerais e permanentes de uma organização, pelo que é produzida pela obtenção e análise de dados similares e constantes, de modo rotineiro e programado.

A *inteligência básica* tenta descrever a visualização de uma imagem fictícia, tão próxima quanto possível de uma real, com a criação de um cenário, logo no início do tratamento da informação respeitante aos factos inalterados. Neste tipo de produto, podemos encontrar os produtos de análise de tendências em que se tem uma forte relação com o planeamento de cenários (Amaral, 2008, p. 266) que são mantidas em base de dados. Mantêm-se continuamente actualizadas e são essencialmente descritivas. Para o efeito, apresentamos um diagrama [figura 3.2], onde as três perspectivas são ilustradas, e prestamos atenção aos níveis de acesso às informações nos sistemas de base de dados, definidos em dois níveis.

Depreendemos ainda que a protecção do ciberespaço acarreta novos e grandes desafios e que, para tal, muito há por fazer, quer no plano nacional, quer internacional. No caso de Angola, há uma estratégia nacional para garantir a segurança do seu ciberespaço, e por via disso, foi promulgada a Lei n.º 7/17, de 16 de Fevereiro, que estabelece o regime jurídico sobre as medidas de protecção das redes e sistemas informáticos, o que de certo modo demonstra preocupação do Estado neste domínio. Por tudo isto, demonstramos a necessidade de acompanhar o desenvolvimento tecnológico com políticas e medidas de combate às novas ameaças que o mundo virtual apresenta, na medida em que a sua aplicação incide fundamentalmente na exploração da base de dados através dos sistemas informáticos.

A Cibersegurança constitui uma ferramenta do Estado para o combate aos crimes cibernéticos, e assim contribui na aplicação da interoperabilidade. Porém, a necessidade de comunicação e de troca de informação electrónica entre serviços similares coloca desafios de cariz técnico, funcional, administrativo e de segurança, especialmente em iniciativas que se mostram transversais entre diferentes áreas de Segurança do Estado. Para que esta necessidade seja colmatada de forma eficiente, mostra-se indispensável que as iniciativas sejam inseridas num contexto comum, onde sejam seguidos um conjunto de regras, normas e princípios orientadores, de forma a garantir que todos os participantes possuam o mesmo suporte e base de entendimento comum a nível técnico, processual e de segurança.

Da análise às funções da interoperabilidade na *intelligence*, concluímos ser imperioso reflectir sobre a questão fundamental para a sua implementação, ou seja, sobre o custo. Não tanto em termos de preço do *software* de base, mas fundamentalmente em despesas de desenvolvimento e de manutenção. É um tipo de *software* altamente sofisticado que requer, para o seu desenho, desenvolvimento e manutenção pessoal com formação adequada.

Portanto, pelo que acima espelhamos, não entraríamos em contradição alguma nem em risco de errar se afirmarmos que a interoperabilidade uma vez implementada na *intelligence* permite economizar tempo, recursos financeiros e racionalizar melhor o capital humano, tornando os Órgãos de Inteligência e de Segurança de Estado mais flexíveis, mais eficientes, mais dinâmicos e mais ágeis no esclarecimento dos fenómenos em pesquisa, contribuindo, oportunamente, com o seu produto, no processo de tomada de decisões políticas do Estado.

REFERÊNCIAS

- ✓ AMARAL, P. C. (2008). *To Secret.* Cruz Quebrada: Academia do Livro.
- ✓ AMARO, António Duarte (2013). Definições e Conceitos em Protecção Civil *in Estudos de Direito e Segurança,* Vol. II (Coord.: Jorge Bacelar Gouveia), Coimbra: Almedina.
- ✓ ANDREW, C., e MITROKHINE (2000). V. *O Arquivo de Mitrokhine. O KGB na Europa e no Ocidente.* Lisboa: D. Qixote..
- ✓ ARON, Raymond (2002). *Paz e Guerra entre as Nações,* 2ª Ed., Brasília: Editora universidade de Brasília,.
- ✓ BAUD, J. (2002). *Encyclopédie du Renseignement et des Services Secrets.* Panazol: Lavauzelle.
- ✓ BESSA, A. M., e PINTO, J. N. (2001). *Introdução à Política - O poder o Estado e classe política.* Lisboa: Editorial Verbo.
- ✓ BESSA, A. M. (2001). *O Olhar de Leviathan. Uma Introdução à Política Externa dos Estados Modernos.* Lisboa: ISCSP.
- ✓ BORAZ, S. C., e BRUNEAU, T. C. (2006). *Reforming Intelligence. Democracy and Effectiveness. Journal of democracy.*
- ✓ BRENNER, S. W., and SCHWERHA, J. J. IV (2004), *Introduction – Cybercrime: A Note on International Issues. International Systems Frontiers 6 (2).*
- ✓ CAETANO, M. (1967). *Manual de Ciência Política e Direito Constitucional* (5ª ed.). Coimbra: Coimbra Editora.
- ✓ CALDEIRA, Carlos Pampulim (2011), *A arte das Bases de Dados,* Lisboa: Edições Silabo.
- ✓ CARDOSO, P. (2004). *As Informações em Portugal.* Lisboa: Gradiva.
- ✓ CARVALHO, J. S. (2006). Segurança Nacional e Informações. *Segurança e Defesa*.
- ✓ CARVALHO, M. P. (2010). *Manual de ciência política e sistemas políticos e constitucionais* (3ª ed.). Lisboa: Quid Juris, sociedade editora.
- ✓ CASTRO, Fabiano Ferreira (2012), *Elementos de Interoperabilidade na Catalogação Descritiva: Configurações contemporâneas para a modelagem de ambientes informacionais digitais, Marília-SP: Universidade Estadual Paulista "Júlio de Mesquita Filho".*

- ✓ CEPIK, M. (2003). *Espionagem e Democracia : agilidade e transparência como dilemas na institucionalização de serviços de inteligência.* Rio de Janeiro: Fundação Getúlio Vargas.
- ✓ CHIAVENATO, I. (2004). *Introdução à Teroria Geral da Administração.* Rio de Janeiro: Elsevier Editora Ltda.
- ✓ CLACK, R. M. (2007). *Intelligence Analysis. A target centric approach.* Washington: C.Q. Press.
- ✓ COUTO, Abel Cabral (1988). *Elementos de Estratégia. Apontamentos para um Curso.* Pedrouços: IAEM.
- ✓ DAVID, Charles-Philippe (2001), *A guerra e a Paz, Abordagem Contemporânea da segurança e da Estratégia,* Lisboa: Instituto Piaget.
- ✓ DAVIS, J. (2009). Strategic Warning: Intelligence support in a world of uncertainty and surprise. In L. K. Johnson, *Handbook of Intelligence Studies* (pp. 173-210). Oxon: Routledge.
- ✓ Dicionário da Língua Portuguesa. (2006). Porto: Porto Editora.
- ✓ DOUGHERTY, J. E., & PFALTZGRAFF, R. J. (2003). *Relações Internacionais - as teorias em confronto* (1ª Ed.), (Traduzido por M. F. Ferreira, M. S. Ferro, & M. J. Ferreira), Lisboa: Gradiva.
- ✓ DUVENAGE, M. A. (2010). *Intelligence Analysis in the Knowledge Age: An Analysis of the Challenges the Practice of Intelligence Analysis.* Unpublished Master Dissertation, University of Stellenbosch, South Africa.
- ✓ ELLIS, W. E. (2010). US Intelligence at the Crossroads. *Mediterranean Quarterly*.
- ✓ ESTEBAN, M. Á. (2007). Reflexiones sobre las fuentes de información abiertas para la produción de Inteligencia Estratégica en los Servicios de inteligencia para la Seguridad. In D. N. Bonilla, M. Á.
- ✓ FREITAS, M. C. (1989). Conceito. In AAVV, *Enciclopédia Luso-Brasileira de Filosofia. Logos.* Lisboa: Editorial Verbo.
- ✓ GARCIA, F. P. (2007). As novas ameaças transnacionais e os espaços mediterrâneos. *Segurança & Defesa*, Lisboa: Universidade Católica.
- ✓ GARCIA, F. P. (2008). A transformação da intelligence. *Segurança & Defesa*, Lisboa: Universidade Católica.
- ✓ GILL, P. (2009). Knowing the self, knowing the other: the comparative analysis of security intelligence. In L. K. Johnson, *Handbook of Intelligence Studies*, Oxon: Routledge.

- ✓ GILL, P., & PHYTHIAN, M. (2009). *Intelligence in an insecure world,* Cambridge: Polity Press.
- ✓ Gizenga, António (2013). *A pertinência dos Órgãos de Inteligência e de Segurança de Estado,* "EAL-Edições de Angola Lda", Instituto de Informações e Seguraça (InIS).
- ✓ GODSON, R. (1995). Covert Action: Neither Exceptional Tool, Nor Magic Bullet. In R. Godson, E. R. May, e G. Schmitt, *U.S. Intelligence at the Crossroads. Agendas for Reform* Washington: Brassey's.
- ✓ GOMES, Henrique Duarte (2013), "Comunicações Electrónicas e Segurança Empresarial" *in Estudos de Direito e Segurança, Vol. II (Coord.: Jorge Bacelar Gouveia),* Coimbra: Almedina.
- ✓ GOOKINS, A. J. (2008). The Role of Intelligence in Policy Making. *SAIS Review*.
- ✓ HEDLEY, J. H. (2009). Analysis for Strategic Intelligence. In L. K. Johnson, *Handbook for Intelligence Studies,* Oxon: Routledge.
- ✓ HERMAN, M. (2004). Intelligence and National Action. In L. K. Johnson, & J. J. Wirtz, *Strategic Intelligence: Windows Into a Secret World,* Los Angeles: Roxbury.
- ✓ HERMAN, M. (2009). *Intelligence in Peace and War* (12ª ed.), Cambridge: University Press.
- ✓ HULNICK, A. S. (2006). What's Wrong with the Intelligence Cycle. *Intelligence and National Security*.
- ✓ JACKSON, P. (2005). Historical Reflections on the Uses and Limits of Intelligence. In P. Jackson, e J. Siegel, *Intelligence and Statecraft: The Use and Limits of Intelligence in International Society,* London: Praeger.
- ✓ JOHNSON, L. K. (2003). Preface to a Theory of Strategic Intelligence. *International Journal of Intelligence and CounterIntelligence*.
- ✓ JOHNSON, L. K., e WIRTZ, J. J. (2004). *Strategic Intelligence. Windows Into a Secret World.* Los Angeles: Roxbury Publishing Company.
- ✓ KAMENSKY, J. M., e BURLIN, T. J. (2004). *Collaboration: Using Networks and Partnerships,* Oxford: Rowman & Littlefield Publishers.
- ✓ KEAN, T. H. (2004). *The 9/11 commission report,* washington: NCTA.
- ✓ KEEGAN, J. (2006). *Espionagem na Guerra. Conhecer o Inimigo: De Napoleão à Al-Qaeda.* Lisboa: Tinta da China.

- ✓ KIRAS, J. D. (2007). The Critical Role of Interagency Cooperation in Countering Suicide Bombings. In J. J. Forest, *Countering Terrorism and Insurgency in the 21st Century. International Perspectives, Volumes 1*, Westport: Praeger Security International.
- ✓ LARA, A. S. (2004). *Ciência Política. Estudo da ordem e da Subversão*, Lisboa: Instituto Superior de Ciências Sociais e Políticas.
- ✓ LEVI, L. (1998). Regime Político. In N. Bobbio, *Dicionário de Política*, Brasília: Universidade de Brasília.
- ✓ LEWIS, D. E. (2003). *Presidents and the politics of agency design: political insulation in the United States government bureaucracy*, Stanford: Stanford University Press.
- ✓ LOWENTHAL, M. M. (2003). *Intelligence, from Secrets to Policy*, Washington D. C.: CQ Press.
- ✓ LOWENTHAL, M. M. (2006). *Intelligence. From Secrets to Policy*, Washington, DC: CQ Press.
- ✓ MAQUIAVEL, N. (2007). *O Príncipe*, Lisboa: Edições Sílabo.
- ✓ MARTIN, Miguel Ángel Ballesteros (2003), «Las estratégias de Seguridad y de defensa», *Fundamentos de la estratégia para el Siglo XXI*, s.d., Centro de estudios de la defensa Nacional.
- ✓ MARTINS, L. (2003), *Direito da Sociedade da Informação, Vol. IV*, Chapter Criminalidade Informática. Coimbra: Coimbra Editores.
- ✓ MINTZ, A., e De ROUEN, K. (2010). *Understanding Foreign Policy Making*, Cambridge: Cambridge University Press.
- ✓ MIRANDA, J. (2002). *Curso de Direito Internacional Público,* Cascais: Principia.
- ✓ MOREIRA, A. (2009). *Ciência Política* (4ª ed.), Coimbra: Almedina.
- ✓ MORUJÃO, A. F. (1985). Função. In AAVV, *Enciclopédia de Filosofia – Logos*, Lisboa: Editorial Verbo.
- ✓ O'BRIEN, K. A. (2007). Covert Action. The "Quiet Option" in International Statecraft. In L. K. Johnson, *Strategic Intelligence* Vol. III, Westport: Praeger Security International.
- ✓ PIRES, C. (1985). Fim. In *Enciclopédia de Filosofia – Logos*, Lisboa: Editorial Verbo.
- ✓ RIBEIRO, António Silva (2010), *Teoria Geral da Estratégia. O essencial ao processo estratégico*, Coimbra: Almedina.
- ✓ ROMANA, H. B. (2004). O novo framework do terrorismo internacional de matriz islâmica: desafios ao modelo de análise em informações estratégicas. In A. Moreira, *Informações e Segurança*, Lisboa: Prefácio.

- ROMANA, Heitor B. (2005). *República Popular da China. A sede do poder estratégico - mecanismos do processo de decisão,* Coimbra: Almedina.
- ROMANA, Heitor B. (2008). Informações: Uma Reflexão Teórica. *Segurança & Defesa,* Coimbra: Almedina.
- RUSS, J. (2000). *Dicionário de Filosofia* Amadora: Didáctica Editora.
- S.A. (1998). Números. In S.A., *Bíblia Sagrada,* Lisboa: Difusora Bíblica.
- SACCHETTI, António Emílio (1986), *Temas de Políticas e Estratégia,* Lisboa: Instituto Superior de Ciências Sociais e Políticas.
- SANTOS, Lino (2013), "Contributos para uma melhor Governação da Cibersegurança em Portugal" *in Estudos de Direito e Segurança, Vol. II (Coord.: Jorge Bacelar Gouveia),* Coimbra: Almedina.
- SCHMID, G. (2001). *On the existence of a global system for the interception of private and commercial communications (ECHELON interception system).* Bruxelas: European Parliament.
- SHULSKY, A. (1995). What is Intelligence? Secrets and Competition Among States. In R. Godson, E. R. May, e G. Schmitt, *U.S. Intelligence at the Crossroads,* Washington: Brassey's.
- SHULSKY, A. N., e SCHMITT, G. J. (2002). *Silent Warfare. Understanding the World of Intelligence*, Dulles, Virginia: Potomac Books.
- SIBERSCHATZ, Abraham; KORTH, Henry F., e SUDARSHAN S. (2010), *Sistema de Banco de Dados,* (Trad. por Marília Guimarães Pinheiro e Cláudio César Canhette). Produtora Editorial: Salete del Guerra, 3ª edição, São Paulo.
- SIMS, Jennifer E. (2009). A Theory of Intelligence and International Politics. In G. F. Treverton, e W. Agrell, *National Intelligence Systems. Current Research and Future Prospects,* Cambridge: Cambridge University Press.
- SOUSA, F. D. (2005). *Dicionário de Relações Internacionais,* Santa Maria da Feira: Edições Afrontamento.
- TREVERTON, G. F. (2003). *Reshaping National intelligence in an age of information,* Cambridge: Cambridge University Press.
- TROY, T. F. (2004). The Quaintness of the U.S. Intelligence Comunity: It's Origin, Theory, and Problems. In L. K. Johnson, e J. J. Wirtz, *Strategic Intelligence. Windows Into a Secret World,* Los Angeles: Roxbury Publishing Company.
- TSU, S. (1974). *A Arte da Guerra,* Lisboa: Edições Sílabo.

- ✓ WALTZ, Edward. (2003). *Knowledge Management in the Intelligence Enterprise*, Norwood: Artech House.
- ✓ WARNER, M. (2009). Building a Theory of Intelligence Systems. In G. F. Treverton, *National Intelligence Systems*, Cambridge: Cambridge University Press.
- ✓ WEINER, T. (2008). *História da CIA - um legado de cinzas*, (P. E. Duarte, Trad.) Lisboa: DIFEL.
- ✓ RIBEIRO, H. M. (2008). *Dicionário de Termos e Citações de Interesse Político e Estratégico, Contributo.* Lisboa: Gradiva.

WEBGRAFIA

- ✓ RIBEIRO, F. P. (2007). *Serviços Secretos e Relações Internacionais: forças de bastidores da política nacional ou um novo campo de estudo para as relações internacionais*, Jornal de Defesa e Relações Internacionais: http://www.jornaldefesa.com.pt/conteudos/view_txt_big.asp?id=477. Consultado em 19 de Setembro de 2010.
- ✓ HANNAH, G., O' Brien, K., & RATHMELL, A. (2005). *Intelligence and security legislation for security sector reform*, RAND Corporation: http://www.rand.org/pubs/technicalreports/2005/RANDTR288.pdf,. Consultado em 11 de Novembro de 2014.
- ✓ HUNTER, T. B. (2007), *The Chalanges of Intelligence Sharing*, Operational Studies: http://www.operationalstudies.com/terrorism/TerrorismIntelligencePaper2.pdf. Consultado em 12 de Novembro de 2015.
- ✓ LIBICKI, M. C. (1995), *What Is Information Warfare?* Washington D.C.: United States Government Printing. http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA367662. Consultado em Janeiro de 2009.
- ✓ RODRIGUES, J. C. (2009). *As Informações Estratégicas. A União Europeia e a Segurança Nacional.* Revista Militar: http://www.revistamilitar.pt/modules/articles/article.php?id=415. Consultado em 22 de Setembro de 2014.
- ✓ PETERSON, M. (2005). *Bureau of Justice Assistance, Office of Justice Programs*, United States Department of Justice: http://www.ncjrs.gov/pdffiles1/bja/210681.pdf,. Consultado em 08 de Dezembro de 2014.

- ✓ Wikipédia, enciclopédia livre *(2008). Interoperabilidade: http://www.<Revista: TransInformação, Campinas,20(2)maio/ago, 2008/> <GooGle Acadêmico - IX Congreso Internacional del CLAD sobre la reforma del estado/> <Site: Governo Eletrônico -/>*. Consultado em 16 de Junho de 2014.
- ✓ Agência para modernização administrativa (IP) (2011), Interoperabilidade na Administração Pública: *Procedimentos para adesão à iAP – Plataforma de interoperabilidade da administração pública*, Versão 3.0, Disponível em www.ama.pt, Consultado em 15.03.2016.
- ✓ DNI. (08 de Março de 2011). *Data Gathering*. Intelligence.gov: http://www.intelligence.gov/about-the-intelligence-community/how-intelligence works/data-gathering.html. Consultado em 16 de Julho de 2015.
- ✓ WILLIAMS, P. D. (2008). *Security Studies. An Introduction,* New York: Routledge, p. 134.
- ✓ ARQUILLA, J. and D. Ronfeldt (Eds.) (2001), *Networks and Netwars: The future of terror, Crime and Militancy.* Santa Mónica. CA: RAND Corporation. http://www.rand.org/pubs/monograph-reports/MR1382.html. Consultado em Julho de 2008.
- ✓ DENNING, D. (2000), *Cyberterrorism – Testimon before the Special Oversight Panel on Terrorism Committee on Armed Services, U.S. House of Representatives.* http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html. Consultado em Setembro de 2007.

LEGISLAÇÃO

- ✓ Constituição da República de Angola.
- ✓ Lei n.º 10/02, de 16 de Agosto, Lei do Segredo do Estado.
- ✓ Lei n.º 11/02, de 16 de Agosto, Lei do Acesso aos Documentos Administrativos.
- ✓ Lei n.º 12/02, de 16 de Agosto, Lei de Segurança Nacional.
- ✓ Lei n.º 22/11, de 17 de Junho, Lei da Protecção de Dados Pessoais.
- ✓ Lei n.º 7/17, de 16 de Fevereiro, Lei da Protecção das Redes e Sistemas Informáticos.
- ✓ Decreto Legislativo Presidencial n.º 5/12, de 15 de Outubro, aprova a Organização e Funcionamento dos Órgãos Auxiliares do Presidente da República.
- ✓ Decretos Presidenciais n.º 201/13, de 02 de Dezembro, aprova o Estatuto Orgânico da Casa de Segurança do Presidente da república.
- ✓ Decretos Presidenciais n.º 108/16, de 25 de Maio, aprova o Regulamento Geral das

Comunicações Electrónicas.

ANEXOS

Lei n.º 10/02, de 16 de Agosto, Lei do Segredo do Estado.

Lei n.º 11/02, de 16 de Agosto, Lei do Acesso aos Documentos Administrativos.

Lei n.º 12/02, de 16 de Agosto, Lei de Segurança Nacional.

Lei n.º 22/11, de 17 de Junho, Lei da Protecção de Dados Pessoais.

Lei n.º 7/17, de 16 de Fevereiro, Lei da Protecção das Redes e Sistemas Informáticos.

Decreto Legislativo Presidencial n.º 5/12, de 15 de Outubro, aprova a Organização e Funcionamento dos Órgãos Auxiliares do Presidente da República.

Decreto Presidencial n.º 201/13, de 02 de Dezembro, aprova o Estatuto Orgânico da Casa de Segurança do Presidente da república.

Decreto Presidencial n.º 108/16, de 25 de Maio, aprova o Regulamento Geral das Comunicações Electrónicas.

ANEXO 1

Sexta-feira, 16 de Agosto de 2002 — I Série — N.º 65

DIÁRIO DA REPÚBLICA

ÓRGÃO OFICIAL DA REPÚBLICA DE ANGOLA

Preço deste número — Kz: 40,00

Toda a correspondência, quer oficial, quer relativa a anúncio e assinaturas do «Diário da República», deve ser dirigida à Imprensa Nacional — U.E.E., em Luanda, Caixa Postal 1306 — End. Teleg.: «Imprensa»	ASSINATURAS	Ano	O preço de cada linha publicada nos Diários da República 1.ª e 2.ª séries é de Kz: 27,50 e para a 3.ª série Kz: 32,50, acrescido do respectivo imposto do selo, dependendo a publicação da 3.ª série de depósito prévio a efectuar na Tesouraria da Imprensa Nacional — U. E. E.
	As três séries	Kz: 95 000,00	
	A 1.ª série	Kz: 55 500,00	
	A 2.ª série	Kz: 32 500,00	
	A 3.ª série	Kz: 21 500,00	

IMPRENSA NACIONAL-U.E.E.

Rua Henrique de Carvalho n.º 2
Caixa Postal n.º 1306

CIRCULAR

Excelentíssimos Senhores:

Havendo necessidade de se evitarem os inconvenientes que resultam para os nossos serviços do facto das respectivas assinaturas do *Diário da República* não serem feitas com a devida oportunidade.

Para que não haja interrupção na remessa do *Diário da República* aos estimados clientes, temos a honra de informá-los que estão abertas a partir desta data até 15 de Dezembro de 2002 as assinaturas do *Diário da República* para o ano de 2003 pelo que deverão providenciar o respectivo pagamento.

1. Os preços das assinaturas do *Diário da República* no território nacional passam a ser os seguintes:

As 3 séries	Kz: 165 750,00
1.ª série	Kz: 97 750,00
2.ª série	Kz: 55 250,00
3.ª série	Kz: 38 250,00

2. As assinaturas serão feitas apenas no regime anual.

3. Aos preços mencionados no n.º 1 acrescer-se-á um valor adicional para portes de correio por via normal das três séries, para todo o ano, no valor de Kz: 27 750,00 que poderá sofrer eventuais alterações em função da flutuação das taxas a praticar pela Empresa Nacional de Correios de Angola no ano 2003. Os clientes que optarem pela recepção das suas assinaturas através do correio deverão indicar o seu endereço completo, incluindo a Caixa Postal, a fim de se evitarem atrasos na sua entrega, devolução ou extravio.

Observações:

a) estes preços poderão ser alterados se houver uma desvalorização da moeda nacional, numa proporção superior à base que determinou o seu cálculo.

b) as assinaturas que forem feitas depois de 15 de Dezembro de 2002 sofrerão um acréscimo de uma taxa correspondente a 15%.

c) aos organismos do Estado que não regularizem os seus pagamentos até 15 de Dezembro do ano em curso não lhes serão concedidas a crédito as assinaturas do Diário da República, para o ano 2003.

SUMÁRIO

Decreto executivo conjunto n.º 32/02:

Determina que o número de matrícula dos veículos automóveis do regime de importação temporária será constituído por um grupo de letras ITA sendo as duas primeiras como indicativo do regime de importação e a terceira como indicativo do País e por um grupo de dois algarismos que indica a ordem de série. — Revoga toda a legislação que contrarie o disposto no presente decreto executivo conjunto.

Ministério das Finanças

Despacho n.º 199/02:

Fixa o montante do fundo permanente da Delegação Provincial do Interior do Cunene.

ASSEMBLEIA NACIONAL

Lei n.º 10/02
de 16 de Agosto

O ordenamento jurídico-administrativo angolano, através do Decreto-Lei n.º16-A/95, de 15 de Dezembro, consagra o direito a informação administrativa, o princípio da administração aberta e o princípio da transparência.

Esses direitos, princípios e regras fundamentais não podem colidir com outros bens ou valores, também constitucionalmente tutelados como segurança interna e externa do Estado.

Nesse quadro, o Segredo de Estado, pode ser um elemento de eficácia da própria acção administrativa, sobretudo nos sectores cujo desnudamento ponha em causa a sobrevivência do Estado.

Assim, por um lado, impõe-se um adequado enquadramento do Segredo de Estado em moldes estritamente necessários e controlados, orgânica, política e jurisdicionalmente e, por outro, revogar a Lei n.º 1/83, de 23 de Fevereiro, Lei do Segredo Estatal, por não se conformar com o actual quadro jurídico constitucional.

Nestes termos, ao abrigo da alínea *b)* do artigo 89.º da Lei Constitucional, a Assembleia Nacional aprova a seguinte:

LEI DO SEGREDO DE ESTADO

CAPÍTULO I
Disposições Gerais

ARTIGO 1.º
(Objecto)

1. O regime geral do Segredo de Estado é definido pela presente lei e obedece, dentre outros, aos princípios de justiça, imparcialidade e da prossecução do interesse público, bem como ao dever de fundamentação.

2. As restrições de acesso aos arquivos, processos e registos administrativos e judiciais, por razões atinentes, à investigação criminal ou à intimidade das pessoas, bem como as respeitantes aos serviços de informações e da ordem interna da República de Angola regem-se por legislação própria.

ARTIGO 2.º
(Âmbito, objectivo do segredo)

1. São abrangidos pelo Segredo de Estado os documentos e informações cujo conhecimento por pessoas não autorizadas é susceptível de pôr em risco ou de causar dano à Independência Nacional, à unidade e integridade do Estado e à sua segurança interna e externa.

2. O risco e o dano referidos no número anterior são avaliados, caso a caso, em face das circunstâncias concretas, não resultando automaticamente da natureza das matérias a tratar.

3. Podem ser submetidos ao regime de Segredo de Estado, verificado o condicionalismo previsto no número anterior, os documentos e informações que respeitem as seguintes matérias:

a) as que são transmitidas, a título confidencial, por Estados estrangeiros ou por organizações internacionais;
b) as que regulam o funcionamento das instituições democráticas;
c) as que salvaguardam os direitos, liberdades e garantias dos cidadãos;
d) as que previnam e assegurem a operacionalidade e a segurança do pessoal, dos equipamentos, do material e das instalações das forças armadas e das forças e serviços de segurança;
e) as que cuja divulgação pode facilitar a prática de crimes contra a segurança do Estado;
f) as que pela natureza comercial, industrial, científica, técnica ou financeira interessam à preparação da defesa militar do Estado;
g) as que estejam ligadas a instrumentos críticos de competitividade como os de natureza técnica e científica;
h) as que salvaguardam os interesses financeiros, monetários, económicos e comerciais do Estado;
i) as que defendem o sigilo de dados pessoais cuja divulgação seja interdita pelo titular.

ARTIGO 3.º
(Âmbito, subjectivo do segredo)

1. O Segredo de Estado abrange todas as pessoas, situadas no território nacional ou fora dele, enquadradas ou não na administração pública e que, por qualquer razão, entrem em contacto com matérias consideradas, nos termos da presente lei, Segredo de Estado.

identificando os interesses à proteger e os motivos ou as circunstâncias concretas que justificam a classificação.

2. A classificação no grau de confidencial e reservado deve ser fundamentada no momento em que se limite num caso concreto o acesso a informação ou material com base nessa classificação.

3. A informação e materiais classificados de várias partes destacáveis e aqueles de que possa ser destacada a informação, em razão da qual a classificação foi atribuída, podem ser objecto de classificação parcial ou de classificação das diversas partes com graus diferentes.

4. Caso seja impossível o destaque a que se refere o número anterior, a informação e o material são classificados com o grau mais elevado de entre os atribuídos às várias partes que os constituem.

5. O grau de classificação funda-se unicamente na informação ou material objecto de classificação, independentemente da classificação de outra informação ou material conexo ou mencionado.

ARTIGO 19.º
(Duração da classificação)

1. A duração da classificação de segurança nacional deve-se limitar ao seguinte:

a) não exceder o tempo estritamente necessário;
b) fixar a duração da classificação pela indicação da data, período de tempo ou condição;
c) fixar a decisão sobre a classificação e o grau atribuído a informação ou material;
d) ser renovada de cinco em cinco anos.

2. A duração pode ir até 25 anos.

3. As matérias classificadas de outros Estados ou de organizações internacionais de que a República de Angola faça parte, mantêm os períodos de validade que forem fixados em convenção internacional ou que constem de normas de segurança aos quais Angola se tenha obrigado a dar cumprimento, com base na reciprocidade.

ARTIGO 20.º
(Classificação de urgência)

1. Se por razão de urgência for necessário classificar um documento como segredo de Estado, têm competência para fazê-lo, provisoriamente, no âmbito da sua competência, com obrigatoriedade de comunicar no mais curto prazo para ratificação, às autoridades com competência originária para classificá-los:

a) o Chefe do Estado Maior General das Forças Armadas Angolanas;
b) o Director Geral do Serviço de Inteligência Externa;
c) o Chefe do Serviço de Informações;
d) o Chefe do Serviço de Inteligência Militar.

2. A competência a que se refere o número anterior do presente artigo, não é delegável.

3. Decorridos 10 dias, contados da data da classificação provisória, se esta não for ratificada, opera-se a caducidade.

CAPÍTULO V
Protecção das Matérias Classificadas

ARTIGO 21.º
(Acesso)

1. Têm acesso a informação e materiais classificados as pessoas credenciadas, nos termos do regime de credenciação de segurança nacional, com grau igual ou superior ao grau de classificação.

2. As pessoas credenciadas apenas podem ter acesso a informação e materiais classificados que necessitem de conhecer para o exercício das suas funções.

ARTIGO 22.º
(Dever de sigilo)

1. As pessoas que tenham acesso a informação e materiais classificados estão sujeitas ao dever de sigilo.

2. Para os funcionários e agentes da administração pública a violação do dever de sigilo constitui ilícito disciplinar, independentemente da acção penal a que haja lugar, nos termos da Lei Penal.

ARTIGO 23.º
(Dever de protecção)

Quem constatar o acesso não autorizado a informação ou materiais classificados ou susceptíveis de classificação deve providenciar a sua imediata protecção e a comunicação do facto às entidades competentes.

ARTIGO 24.º
(Violação dolosa de segredo de Estado)

1. O titular de cargo político ou funcionário público que, mesmo depois de deixar de o ser, revelar segredo de Estado que lhe tenha sido confiado em virtude das suas funções, com intenção de prejudicar o Estado ou a terceiro, ou ainda de obter para si ou para outrem um benefício ilegítimo, deve ser punido com a pena de prisão de 6 meses a 2 anos, se o prejuízo efectivamente ocorrer.

2. Se o prejuízo não se verificar a pena de prisão deve ser até 1 ano.

3. A mesma pena, atenuada, deve ser aplicada em caso de tentativa.

4. Ao titular de cargo político ou funcionário público pode ser aplicada cumulativamente a pena de demissão, nos termos dos artigos 57.º e 65.º do Código Penal.

ARTIGO 25.º
(Violação negligente de segredo de Estado)

O titular de cargo político ou funcionário público que, por negligência revelar ou possibilitar que outrem revele segredo de Estado que lhe tenha sido confiado em virtude das suas funções, deve ser punido com a pena de prisão até 6 meses.

ARTIGO 26.º
(Divulgação não autorizada)

Todo aquele que sem ser titular de cargo político ou funcionário público tiver acesso a informação e materiais classificados, independentemente da forma e da fonte e proceder à sua divulgação pública sem que para tal tenha sido autorizado pela entidade competente, fica sujeito as penas estabelecidas nos artigos 24.º e 25.º da presente lei, consoante actue com dolo ou negligência.

ARTIGO 27.º
(Efeito das penas aplicadas a titular de cargo político)

A condenação definitiva por crime de violação de segredo de Estado ao titular de cargo político implica a perda do respectivo mandato, com as consequências previstas na Lei Constitucional.

CAPÍTULO VI
Credenciação

ARTIGO 28.º
(Credenciação de segurança nacional)

1. A credenciação de segurança nacional é o acto mediante o qual é autorizado o acesso, sem prejuízo do princípio da necessidade de conhecer, a informação e os materiais classificados, definidos no regime de classificação de segurança nacional.

2. A credenciação pressupõe uma avaliação e uma decisão sobre a idoneidade de determinada pessoa para ter acesso a informação e a materiais classificados, atentos os interesses que fundamentam a existência da classificação.

3. Consideram-se credenciados, independentemente de qualquer procedimento, o Presidente da República, Presidente da Assembleia Nacional, Primeiro-Ministro, membros do Governo, Procurador Geral da República e os Governadores Provinciais.

4. A decisão negativa sobre a credenciação determina a proibição de acesso a informação e a materiais classificados.

ARTIGO 29.º
(Âmbito subjectivo e objectivo)

O regime de credenciação de segurança nacional aplica-se a pessoas singulares de nacionalidade angolana e a pessoas colectivas com sede estatutária ou sede principal e efectiva em Angola e que tenham acesso a informação e materiais classificados, de acordo com o regime de classificação de segurança nacional.

ARTIGO 30.º
(Princípios gerais)

1. O procedimento de credenciação de segurança nacional submete-se aos princípios da legalidade, igualdade, proporcionalidade, imparcialidade e da boa fé, bem como aos demais a que se encontra sujeita a acção administrativa.

2. O procedimento de credenciação de segurança nacional rege-se pelo rigoroso respeito pelos direitos, liberdades e garantias dos cidadãos.

ARTIGO 31.º
(Informação, esclarecimento e consentimento)

O procedimento de credenciação de segurança nacional pressupõe à informação e o esclarecimento, pessoal ou documental, das pessoas que se habilitem à credenciação e o seu consentimento por escrito.

ARTIGO 32.º
(Obrigações do credenciado)

A pessoa individual ou colectiva a quem tenha sido concedida uma credenciação de segurança nacional fica obrigada:

a) ao dever de sigilo e de protecção da informação e materiais classificados;

b) a respeitar o princípio da necessidade de conhecer;

c) a cumprir as normas aplicáveis à classificação e credenciação de segurança nacional e aos procedimentos de segurança, bem como a manter-se actualizada sobre as mesmas;

d) a cumprir as instruções, emitidas pelos órgãos competentes, sobre a segurança da informação e materiais classificados;

e) a manter actualizados os dados que tenha declarado no processo de habilitação;

f) a participar às entidades competentes, quaisquer factos que indiciem falhas ou quebras de segurança, bem como do possível comprometimento da informação classificada.

CAPÍTULO VII
Fiscalização Política do Segredo de Estado

ARTIGO 33.º
(Fiscalização pela Assembleia Nacional)

A Assembleia Nacional fiscaliza, nos termos da Lei onstitucional, do seu Regimento Interno e do artigo 30.º a Lei de Segurança Nacional, o regime do Segredo de stado fixado pela presente lei.

CAPÍTULO VIII
Disposições Finais e Transitórias

ARTIGO 34.º
(Comissão de Fiscalização)

Compete a Comissão de Fiscalização do Acesso aos ocumentos Administrativos, criada pela Lei de Acesso aos ocumentos Administrativos, apreciar as queixas que lhe jam dirigidas sobre dificuldades ou recusa no acesso à formação e materiais classificados, nos termos da presente i e sobre elas emitir parecer.

ARTIGO 35.º
(Instruções nacionais de segurança)

As instruções nacionais de segurança que especificam os ocedimentos e as medidas de segurança para classificação rotecção da informação ou materiais classificados e ainda ra a sua difusão junto de outros Estados e organizações ternacionais, devem ser aprovadas por resolução do nselho de Ministros, no prazo de 120 dias a contar data da entrada em vigor da presente lei.

ARTIGO 36.º
(Procedimento de credenciação)

Os termos em que se processa a credenciação de segurança nacional são definidos por decreto-lei, no prazo de 120 dias a contar da data da entrada em vigor da presente lei.

ARTIGO 37.º
(Acordos de segurança)

O Governo pode celebrar acordos de cooperação sobre segurança em matéria de classificação e materiais classificados, bem como em matéria de credenciação.

ARTIGO 38.º
(Revogação)

É revogada a Lei n.º 1/83, de 23 de Fevereiro, Lei do Segredo Estatal, bem como toda a demais legislação que contrarie o disposto na presente lei.

ARTIGO 39.º
(Dúvidas e omissões)

As dúvidas e omissões que se suscitarem da interpretação e aplicação da presente lei, são resolvidas pela Assembleia Nacional.

ARTIGO 40.º
(Regulamentação)

A presente lei deve ser regulamentada no prazo de 120 dias a contar da data da sua entrada em vigor.

ARTIGO 41.º
(Entrada em vigor)

A presente lei entra em vigor 60 dias a contar da data da sua publicação.

Vista e aprovada pela Assembleia Nacional, em Luanda, aos 18 de Julho de 2002.

O Presidente em exercício da Assembleia Nacional, *Julião Mateus Paulo.*

Promulgada, aos 29 de Julho de 2002.

Publique-se.

O Presidente da República, José Eduardo dos Santos.

ANEXO 2

Lei n.º 11/02
de 16 de Agosto

O Decreto-Lei n.º 16-A/95, de 15 de Dezembro, consagra o direito à informação administrativa que compreende o acesso aos documentos não classificados, certidões ou reproduções autenticadas e aos documentos nominativos relativos a terceiros.

O Estado democrático e de direito assenta no princípio da administração aberta como regra e estabelece as excepções relativas a matéria qualificada como segredo de Estado.

Daí a necessidade de se concretizar e desenvolver o princípio constitucional da democracia participativa que exige da administração pública a prática da transparência administrativa e da sua sujeição ao controlo, bem como de se regular o acesso dos cidadãos aos documentos administrativos.

Nestes termos, ao abrigo da alínea *b*) do artigo 89.º da Lei Constitucional, a Assembleia Nacional aprova a seguinte:

LEI DE ACESSO AOS DOCUMENTOS ADMINISTRATIVOS

CAPÍTULO I
Disposições gerais

ARTIGO 1.º
(Administração aberta)

O acesso dos interessados aos documentos administrativos é assegurado pela administração pública de acordo com os princípios da publicidade, transparência, igualdade, justiça, imparcialidade, colaboração, participação, prossecução do interesse público e do respeito pelos direitos e interesses legalmente protegidos.

ARTIGO 2.º
(Objectivo)

1. A presente lei regula o acesso a documentos relativos a actividades desenvolvidas pelas entidades referidas no seu artigo 3.º

2. O regime de exercício do direito dos cidadãos a serem informados pela administração sobre o andamento dos processos em que sejam directamente interessados e a conhecer as resoluções definitivas que sobre eles forem tomadas consta de legislação própria.

ARTIGO 3.º
(Âmbito)

Os documentos a que se reporta o artigo seguinte são os que têm origem ou são detidos por órgãos do Estado que exerçam funções administrativas e órgãos dos institutos públicos e das associações e outras entidades no exercício de poderes de autoridade, nos termos da Lei.

ARTIGO 4.º
(Definições)

1. Para efeito do disposto na presente lei, são considerados:

a) documentos administrativos: quaisquer suportes de informação gráficos, sonoros, visuais, informáticos ou registos de outra natureza, elaborados ou detidos pela administração pública, directa, indirecta e autónoma designadamente processos, relatórios, estudos, pareceres, actas, autos, circulares, ofícios-circulares, ordens de serviço, despachos normativos internos, instruções e orientações de interpretação legal ou outros elementos de informação;

b) documentos nominativos: quaisquer suportes de informação que contenham dados pessoais;

c) dados pessoais: informações sobre pessoas singulares, identificadas ou identificáveis, que contenham apreciações, juízo de valores ou sejam abrangidas pela reserva da intimidade da vida privada.

2. Não se consideram documentos administrativos, para efeitos da presente lei:

a) as notas pessoais, esboços, apontamentos e outros registos de natureza semelhante;

b) os documentos cuja elaboração não releve da actividade administrativa, designadamente referentes à reunião do Conselho de Ministros, bem como à sua preparação.

ARTIGO 5.º
(Segurança interna e externa)

1. Os documentos que contenham informações cujo conhecimento seja avaliado como podendo pôr em risco ou causar dano à segurança interna e externa do Estado ficam sujeitos a interdição de acesso ou a acesso sob autorização, durante o tempo estritamente necessário, através da classificação nos termos de legislação específica.

2. Os documentos a que se refere o número anterior podem ser livremente consultados, nos termos da presente lei, após a sua desclassificação ou o decurso do prazo de validade do acto de classificação.

ARTIGO 6.º
(Segredo de justiça)

O acesso a documentos referentes a matérias em segredo de justiça é regulado por legislação própria.

CAPÍTULO II
Direito de Acesso

ARTIGO 7.º
(Direito de acesso)

1. Todos têm direito à informação mediante o acesso a documentos administrativos de carácter não nominativo.

2. O direito de acesso aos documentos nominativos é reservado à pessoa a quem os dados digam respeito e a terceiros que demonstrem interesse directo e pessoal, nos termos do artigo seguinte.

3. O direito de acesso aos documentos administrativos compreende não só o direito de obter a sua reprodução, bem como o direito de ser informado sobre a sua existência e conteúdo.

4. O depósito dos documentos administrativos em arquivos não prejudica o exercício, a todo o tempo, do direito de acesso aos referidos documentos.

5. O acesso a documentos constantes de processos não concluídos ou a documentos preparatórios de uma decisão é diferido até à tomada da decisão, ao arquivamento do processo ou ao decurso de um ano após a sua elaboração.

6. O acesso aos inquéritos e sindicâncias tem lugar após o decurso do prazo para eventual procedimento disciplinar.

7. O acesso aos documentos notariais e registrais, aos documentos de identificação civil e criminal, dados pessoais com tratamento automatizado em arquivos históricos rege-se por legislação própria.

ARTIGO 8.º
(Acesso aos documentos nominativos)

1. O direito de acesso a dados pessoais contidos em documentos administrativos é exercido, com as necessárias adaptações nos termos da lei aplicável ao tratamento autorizado de dados pessoais.

2. As informações de carácter médico só são comunicadas ao interessado por intermédio de um médico por si designado.

3. O acesso de terceiro a dados pessoais pode ainda ser autorizado nos seguintes casos:

a) mediante autorização escrita da pessoa a quem os dados se refiram;
b) quando a comunicação dos dados pessoais tenha em vista salvaguardar o interesse legítimo da pessoa a que respeitem e esta se encontre impossibilitada de conceder autorização, e desde que obtido o parecer previsto no número anterior.

4. Podem ainda ser comunicados a terceiros os documentos que contenham dados pessoais quando, pela sua natureza, seja possível aos serviços expurgá-los desses dados sem terem de reconstruir os documentos e sem perigo de fácil identificação.

ARTIGO 9.º
(Correcção de dados pessoais)

1. O direito de rectificar, completar ou suprimir dados pessoais inexactos, insuficientes ou excessivos é exercido nos termos do disposto na legislação referente aos dados pessoais com tratamento automatizado e com as necessárias adaptações.

2. Só a versão corrigida dos dados pessoais é passível de uso ou comunicação.

ARTIGO 10.º
(Uso ilegítimo de informações)

1. É vedada a utilização de informações com desrespeito dos direitos de autor e dos direitos de propriedade industrial, assim como a reprodução, difusão e utilização destes documentos e respectivas informações que possam configurar práticas de concorrência desleal.

2. Os dados pessoais comunicados a terceiros não podem ser utilizados para fins diversos dos que determinaram o acesso, sob pena de responsabilidade por perdas e danos, nos termos legais.

ARTIGO 11.º
(Publicação de documentos)

1. A administração pública deve publicar, por forma adequada:

a) todos os documentos, despachos normativos internos, circulares e orientações, que comportem enquadramento da actividade administrativa;

ANEXO 3

Nestes termos, ao abrigo da alínea *b*) do artigo 88.° da Lei Constitucional, a Assembleia Nacional aprova, a seguinte:

LEI DE SEGURANÇA NACIONAL

CAPÍTULO I
Princípios Gerais

ARTIGO 1.°
(Definição e fins de segurança nacional)

1. A segurança nacional é a actividade do Estado para garantir a ordem, a segurança e a tranquilidade pública e contribuir, assegurar o normal funcionamento das instituições democráticas, o regular exercício dos direitos, liberdades e garantias fundamentais dos cidadãos e o respeito pela legalidade democrática.

2. A actividade de segurança nacional exerce-se nos termos da lei, designadamente, da Lei Penal e Processual Penal, e dos diplomas que estabelecem a organização e funcionamento dos serviços públicos de informações e dos órgãos e serviços de ordem interna da República de Angola.

3. Para prossecução dos fins de segurança nacional, os serviços e órgãos integrados no sistema de segurança nacional devem:

a) produzir informações destinadas a suportar as políticas de segurança e protecção da vida, integridade e dignidade humanas;

b) produzir informações destinadas à salvaguardar a preservação da independência nacional, soberania, a paz e tranquilidade pública bem como a ordem constitucional;

c) realizar acções e produzir informações destinadas a prevenção geral e especial, a protecção contra o terrorismo, a sabotagem, o açambarcamento, a espionagem, o tráfico ilícito de drogas e de substâncias psicotrópicas.

ARTIGO 2.°
(Princípios fundamentais)

1. A actividade de segurança nacional deve pautar-se pela observância das regras gerais de polícia e com respeito pelos direitos, liberdades e garantias e pelos demais princípios do Estado democrático de direito.

2. As medidas de polícia e segurança são as previstas nas leis, não devendo ser utilizadas, para além do estritamente necessário.

3. A prevenção dos crimes contra a segurança do Estado só pode fazer-se com observância das regras gerais sobre polícia e com respeito pelos direitos, liberdades e garantias dos cidadãos.

4. O regime dos órgãos e serviços públicos de segurança deve ser fixado por lei, sendo a organização de cada uma delas únicas para todo o território nacional.

ARTIGO 3.°
(Política de segurança nacional)

A política de segurança nacional consiste no conjunto de princípios, orientações e medidas tendentes a prossecução permanente dos fins definidos no artigo 1.° da presente lei.

ARTIGO 4.°
(Âmbito territorial)

1. A segurança nacional desenvolve-se em todo espaço sujeito aos poderes de jurisdição do Estado angolano.

2. No quadro dos compromissos internacionais e das normas aplicáveis do direito internacional, os órgãos e serviços públicos de segurança podem actuar fora do espaço referido no número anterior em cooperação com os serviços de Estados estrangeiros ou com organizações internacionais de que Angola seja parte.

ARTIGO 5.°
(Deveres gerais especiais de colaboração)

1. Os cidadãos têm o dever de colaborar na prossecução dos fins de segurança nacional, observando as disposições estabelecidas na lei.

2. Os funcionários e agentes do Estado ou das pessoas colectivas públicas, bem como os órgãos de gestão das empresas públicas têm o dever especial de colaboração com os serviços de informações.

3. Os indivíduos investidos nas funções de direcção, chefia, inspecção ou fiscalização em órgãos ou serviços da administração pública têm o dever de comunicar aos serviços de informações competentes os factos de que tomem conhecimento no exercício das suas funções, ou por causa delas, e que constituam preparação, tentativa ou execução de crimes contra a Segurança do Estado.

4. A violação do disposto nos n.os 2 e 3 do presente artigo implica responsabilidade disciplinar e criminal, nos termos da lei.

ARTIGO 6.º
(Garantia de protecção aos colaboradores)

1. Todo o cidadão nacional ou estrangeiro que colabore com os Serviços de Informação e outros serviços especializados em matéria de segurança de Estado, deve gozar de protecção do Estado.

2. Os funcionários e agentes do Estado ou as pessoas colectivas públicas, bem como os órgãos de gestão das empresas públicas que colaborem com os Serviços de Informação e outros serviços especializados em matéria de segurança de Estado, devem gozar de protecção do Estado.

ARTIGO 7.º
(Apartidarismo)

Os órgãos e serviços do Sistema de Segurança Nacional são apartidários.

CAPÍTULO II
Sistema de Segurança Nacional

ARTIGO 8.º
(Órgãos incumbidos da actividade de segurança nacional)

1. A actividade de segurança nacional é exercida através dos órgãos e serviços públicos de informações e os órgãos e serviços da ordem interna previstos na presente lei.

2. A actividade dos serviços públicos de informações e os órgãos e serviços de ordem interna está sujeito a fiscalização política, administrativa e judicial nos termos da Lei Constitucional e da presente lei.

ARTIGO 9.º
(Coordenação e cooperação dos órgãos e serviços públicos de informação e ordem interna)

1. Os órgãos e serviços públicos do sistema de segurança nacional exercem a sua actividade de acordo com os objectivos e finalidades da política de segurança nacional e dentro dos limites do respectivo enquadramento orgânico, o qual respeita o disposto na presente lei.

2. Sem prejuízo do disposto no número anterior, os órgãos e serviços públicos do sistema de segurança nacional cooperam entre si, designadamente, através da comunicação recíproca de dados não sujeitos a regime especial de reserva ou protecção que, não interessando apenas a prossecução dos objectivos específicos de cada serviço, sejam necessários a realização das finalidades de cada um dos outros.

ARTIGO 10.º
(Comunidade de inteligência)

Pela presente lei, é instituída a comunidade de inteligência angolana, integrando no seu seio os órgãos e serviços públicos de informação previstos nas alíneas *f*), *g*) e *h*) do artigo 12.º da presente lei e a sua actividade deve ser regulamentada por diploma próprio.

ARTIGO 11.º
(Segredo de Estado)

O regime do Segredo de Estado é regulado por lei própria.

CAPÍTULO III
Orgânica do Sistema de Segurança Nacional

ARTIGO 12.º
(Órgãos e serviços públicos integrados no Sistema de Segurança Nacional)

Para a prossecução das finalidades e objectivos previstos na presente lei, são criados:

a) o Conselho Superior de Segurança Nacional (CSSN);

b) a Comissão Executiva do Conselho Superior de Segurança Nacional (CSSN);

c) os órgãos e serviços da Ordem Interna do Ministério do Interior;

d) órgãos e serviços do Sistema de Autoridade Marítima;

e) os órgãos e serviços do Sistema de Autoridade Aeronáutica;

f) o Serviço de Inteligência Externa (SIE);

g) o Serviço de Informações (SINFO);

h) o Serviço de Inteligência Militar (SIM);

ARTIGO 13.º
(Natureza)

Todas as instituições referidas no artigo anterior integram o Sistema de Segurança Nacional e têm a natureza de serviços públicos.

ARTIGO 14.º
(Autonomia)

Os serviços públicos referidos nas alíneas *f*) e *g*) do artigo 12.º são dotados de autonomia administrativa e financeira e possuem património próprio.

f) ordenar a suspensão da actividade de empresas, grupos, organizações que se dediquem a acções de criminalidade organizada, designadamente, de sabotagem, espionagem ou terrorismo ou a preparação, treino ou recrutamento de pessoas para aqueles fins.

2. As medidas previstas no número anterior devem ser ediatamente comunicadas ao Tribunal competente e reciadas pelo juiz, em ordem a sua validade.

3. Os agentes ou funcionários da polícia não unifor-izados que, nos termos da lei, ordenem a identificação de ssoas ou emitam qualquer outra ordem ou mandato gítimo, devem previamente fazer prova da sua qualidade polícia.

4. Os funcionários ou agentes civis ou militares dos rviços de Informações previstos na presente lei não dem exercer poderes, praticar actos ou desenvolver tividades do âmbito ou competências específicas dos ibunais ou das entidades com funções policiais.

5. É expressamente proibido aos funcionários e agentes, vis ou militares, do Serviço de Informações proceder detenção de qualquer indivíduo ou instruir processos nais.

ARTIGO 24.º
(Controle de comunicações)

1. A decisão sobre o controle de comunicações compete Juiz Conselheiro da Câmara Criminal do Tribunal premo a quem o processo for distribuído a requerimento s órgãos e serviços públicos de informações bem como s forças e serviços de ordem interna.

2. Os órgãos e serviços públicos de informações e os gãos e serviços de ordem interna do Sistema de Segurança acional requerem a autorização por iniciativa própria e vidamente fundamentada.

3. A decisão a que se refere o n.º 1 do presente artigo ve ser proferida num prazo não superior a 72 horas a ntar da data da solicitação e, é válida por um período não perior a 45 dias, podendo ser prorrogado por iguais ríodos após solicitação expressa dos competentes órgãos r Sistema de Segurança Nacional.

ARTIGO 25.º
(Centro de Processamento de Dados)

1. Os órgãos e serviços do Sistema de Segurança Nacional, podem dispor de Centros de Processamentos de Dados, compatíveis com a natureza dos serviços, aos quais competem processar e conservar em arquivos apropriados os dados e informações recolhidas no âmbito da sua actividade.

2. Os Centros de Processamento de Dados são criados de forma compartimentada com base na natureza específica de cada um dos órgãos e serviços do Sistema de Segurança Nacional.

ARTIGO 26.º
(Funcionamento)

1. Os critérios e normas técnicas necessárias ao funcionamento dos Centros de Processamento de Dados, bem como os regulamentos indispensáveis a garantia da segurança das informações processadas, são aprovados pelo Conselho de Ministros sob proposta do Conselho Superior de Segurança Nacional.

2. Os Centros de Processamento de Dados só podem iniciar a sua actividade depois de publicada a regulamentação a que se refere o número anterior.

ARTIGO 27.º
(Acesso de funcionários e agentes aos dados)

1. Os funcionários e agentes, civis ou militares, só podem ter acesso a dados e informações conservados no Centro de Processamento de Dados desde que autorizados pelos respectivos superiores hierárquicos, sendo proibida a sua utilização com finalidades diferentes da defesa do Estado democrático de direito ou da prevenção e repressão da criminalidade.

2. O funcionário ou agente, civil ou militar que comunicar ou fizer uso de dados e informações com violação do disposto no número anterior é punido com prisão até 3 anos, se pena mais grave não lhe for aplicável e sem prejuízo da medida disciplinar que ao caso couber.

3. Sem prejuízo dos poderes de fiscalização previsto no artigo 29.º da presente lei, nenhuma entidade estranha aos Serviços de Informações e as forças e órgãos de segurança interna pode ter acesso directo aos dados e informações conservadas no centro de dados.

X

ARTIGO 28.º
(Cancelamento e rectificação de dados)

1. Se no decurso de um processo judicial ou administrativo se produzir erro na imputação de dados ou informações ou se verificar alguma irregularidade no seu tratamento, a entidade processadora fica obrigada a dar conhecimento do facto a Conselho de Fiscalização, prevista no artigo 31.º da presente lei.

2. Quem, por acto de qualquer funcionário ou agente de autoridade ou no decurso de processo judicial ou administrativo, tiver conhecimento de dados que lhe digam respeito e que considere erróneos, irregularmente obtidos ou violadores dos seus direitos, liberdades e garantias pessoais pode, sem prejuízo do direito ao recurso às outras garantias legais, requerer a Conselho de Fiscalização, que proceda às verificações necessárias e ordene o seu cancelamento ou a rectificação dos dados que se mostrarem incompletos ou erróneos.

ARTIGO 29.º
(Autonomia dos Centros de Processamento de Dados)

Os Centros de Processamento de Dados de cada um dos serviços de segurança que integram o Sistema de Segurança Nacional, são autónomos e compatíveis com a natureza específica de cada um dos serviços.

CAPÍTULO IV
Fiscalização Política

ARTIGO 30.º
(Conselho de Fiscalização)

1. Sem prejuízo dos poderes de fiscalização da Assembleia Nacional, nos termos constitucionais, o controlo do Serviço de Informações, dos Serviços de Inteligência Externa e Militar do Sistema de Segurança Nacional é assegurado por um Conselho de Fiscalização à eleger pela Assembleia Nacional.

2. O Conselho a que se refere o número anterior é composto por cinco Deputados eleitos de acordo ao princípio da proporcionalidade, por maioria absoluta dos Deputados presentes e no âmbito funcional da Comissão competente da Assembleia Nacional.

3. A eleição dos membros da Comissão de Fiscalização é nominal e válida por um período de 4 anos, só interrompível por deliberação da Assembleia Nacional, tomada nos mesmos termos.

ARTIGO 31.º
(Competência)

1. Os Serviços de Informações, de Inteligência Externa e Militar do Sistema de Segurança Nacional, devem submeter anualmente à Assembleia Nacional através do Conselho de Fiscalização, os relatórios de actividade.

2. O Conselho de Fiscalização, tem o direito de requerer e obter dos serviços e órgãos do Sistema de Segurança Nacional, através dos titulares, os esclarecimentos complementares aos relatórios que considere necessários ao cabal exercício dos seus poderes de fiscalização.

3. O Conselho de Fiscalização deve apresentar anualmente à Assembleia Nacional, o parecer sobre o funcionamento dos serviços que constituem a Comunidade de Inteligência Angolana.

ARTIGO 32.º
(Posse e renúncia)

1. Os membros do Conselho de Fiscalização, tomam posse perante o Presidente da Assembleia Nacional, no prazo de 15 dias a contar da publicação do resultado da eleição.

2. Os membros do Conselho de Fiscalização podem renunciar ao mandato mediante declaração escrita apresentada ao Presidente da Assembleia Nacional, a qual deve ser publicada na 2.ª série do *Diário da República*.

ARTIGO 33.º
(Deveres)

1.Constituem deveres especiais dos membros do Conselho de Fiscalização:

a) exercer o cargo com a independência, isenção e sentido de missão inerentes à função que exercem;

b) contribuir, pelo seu zelo, dedicação e exemplo, para a aplicação da presente lei;

c) guardar sigilo nos termos do regime do Segredo de Estado;

d) observar um elevado sentido de Estado.

2. O dever de sigilo referido no número anterior mantém-se após a cessação dos respectivos mandatos.

ANEXO 4

Sexta-feira, 17 de Junho de 2011 — I Série — N.º 114

DIÁRIO DA REPÚBLICA

ÓRGÃO OFICIAL DA REPÚBLICA DE ANGOLA

Preço deste número — Kz: 220,00

Toda a correspondência, quer oficial, quer relativa a anúncio e assinaturas do «*Diário da República*», deve ser dirigida à Imprensa Nacional — E. P., em Luanda, Caixa Postal 1306 — End. Teleg.: «Imprensa»

ASSINATURAS

	Ano
As três séries	Kz: 440 375,00
A 1.ª série	Kz: 260 250,00
A 2.ª série	Kz: 135 850,00
A 3.ª série	Kz: 105 700,00

O preço de cada linha publicada nos *Diários da República* 1.ª e 2.ª séries é de Kz: 75,00 e para a 3.ª série Kz: 95,00, acrescido do respectivo imposto do selo, dependendo a publicação da 3.ª série de depósito prévio a efectuar na Tesouraria da Imprensa Nacional — E. P.

SUMÁRIO

ASSEMBLEIA NACIONAL

Lei n.º 22/11

de 17 de Junho

A protecção dos dados pessoais, da confidencialidade e da reserva da vida privada assume uma relevância fundamental no contexto da salvaguarda dos direitos fundamentais dos cidadãos, reconhecidos pela Declaração Universal dos Direitos do Homem e pela Carta Africana dos Direitos do Homem e dos Povos.

A consagração, na Constituição da República de Angola, do direito à reserva da vida privada e da possibilidade do recurso à providência «habeas data» representa manifestamente um grande passo na adopção de um quadro legislativo nesta matéria.

O direito à privacidade traduz-se também no respeito pela reserva da vida privada dos cidadãos face ao tratamento de dados pessoais que lhes digam respeito. Muito embora tal tratamento tenha um papel relevante para a melhoria do bem-estar dos cidadãos e para o progresso económico num contexto de dinamização e de desenvolvimento de uma maior variedade de serviços, nomeadamente no âmbito das tecnologias e da sociedade da informação, há que assegurar que o mesmo seja efectuado num contexto de respeito pela sua privacidade.

A Assembleia Nacional aprova, por mandato do povo, nos termos do n.º 2 do artigo 165.º e da alínea *d*) do n.º 2 do artigo 166.º, ambos da Constituição da República de Angola, a seguinte:

LEI DA PROTECÇÃO DE DADOS PESSOAIS

CAPÍTULO I
Disposições Gerais

ARTIGO 1.º
(Objecto)

A presente lei tem por objecto estabelecer as regras jurídicas aplicáveis ao tratamento de dados pessoais com o objectivo de garantir o respeito pelas liberdades públicas e os direitos e garantias fundamentais das pessoas singulares.

ARTIGO 2.º
(Âmbito de aplicação objectiva)

A presente lei aplica-se ao tratamento de dados pessoais efectuado por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de

ocasião da transacção realizada e se não implicar para o destinatário dispêndio adicional ao custo do serviço de telecomunicações.

3. No caso previsto no número anterior, o titular dos dados tem o direito de se opor ao seu tratamento para os fins constantes deste artigo.

4. Para os efeitos do disposto no número anterior, o titular deve ter acesso a meios que lhe permitam a qualquer momento recusar, sem ónus, gratuitamente e independentemente de justa causa, o envio dessa publicidade para o futuro.

5. Em caso de oposição, as entidades que promovam o envio de mensagens publicitárias devem manter uma lista actualizada, por si ou por organismos que as representem, de titulares que manifestaram a sua oposição ao envio de tais mensagens.

6. O tratamento de dados para os fins previstos no n.º 2 anterior não requer notificação à Agência de Protecção de Dados, nem consentimento dos titulares dos dados.

7. Com vista a maior eficácia do disposto no n.º 2 do presente artigo, a Agência de Protecção de Dados apoia a constituição de listas de titulares que manifestem a sua oposição ao envio de mensagens publicitárias.

8. O responsável pelo tratamento de dados pessoais para os fins constantes deste artigo deve informar o destinatário:

a) sobre a procedência dos seus dados pessoais, no caso de os mesmos terem origem em fontes acessíveis ao público;
b) de que os seus dados serão comunicados a destinatários para fins de marketing directo ou utilizados por conta de terceiros, caso o titular dos dados tenha consentido, observando-se nesse caso os requisitos aplicáveis à comunicação de dados constantes do artigo 21.º;
c) sobre a identidade do responsável pelo tratamento, sendo proibido o envio de publicidade ocultando ou dissimulando a identidade da pessoa em nome de quem é efectuada a comunicação.

ARTIGO 20.º

(Requisitos específicos para a gravação de chamadas)

1. A gravação de chamadas é admitida quando realizada no âmbito de práticas comerciais lícitas, para o efeito de prova de uma transacção comercial, desde que:

a) o titular dos dados tenha dado previamente o seu consentimento expresso e inequívoco à gravação, devendo esta iniciar com o registo do consentimento;
b) a Agência de Protecção de Dados tenha autorizado tal tratamento.

2. Exceptua-se da necessidade de consentimento do titular dos dados e da autorização prévia da Agência de Protecção de Dados, as gravações de comunicações de e para serviços públicos destinados a prover situações de emergência de qualquer natureza.

3. No caso previsto no número anterior, o tratamento de dados está sujeito a notificação prévia à Agência de Protecção de Dados.

SECÇÃO III

Comunicação e Interconexão de Dados Pessoais

ARTIGO 21.º

(Comunicação de dados)

A comunicação de dados pessoais pelo responsável a um destinatário está sujeito às seguintes regras:

a) se os dados pessoais forem comunicados ao destinatário para efeitos de prossecução de finalidades próprias deste, o destinatário será considerado também responsável pelo tratamento dos mesmos, devendo cumprir as disposições legais que lhe são aplicáveis;
b) se os dados pessoais forem comunicados ao destinatário para efeitos de prossecução das finalidades do responsável que comunica os dados, tratando o destinatário os dados em nome e em representação do responsável, o destinatário é considerado um subcontratado, devendo cumprir as disposições legais que lhe são aplicáveis;
c) se os dados pessoais forem comunicados ao destinatário não se verificando nenhuma das condições constantes dos pontos anteriores nem estando este sob autoridade directa do responsável pelo tratamento ou de subcontratado, o destinatário será considerado um terceiro.

ARTIGO 22.º

(Comunicação de dados a responsável pelo tratamento ou a terceiro)

1. A comunicação de dados a destinatário que seja também responsável pelo tratamento ou que seja um terceiro só pode ser efectuada verificadas as seguintes circunstâncias:

a) consentimento inequívoco e expresso do titular dos dados;

b) notificação à Agência de Protecção de Dados.

2. A comunicação de dados não está sujeita ao prévio consentimento do titular quando:

a) a comunicação decorra de lei ou de decisão judicial;

b) os dados tenham sido recolhidos de fontes acessíveis publicamente em respeito das suas condições de consulta e utilização, aplicáveis a tais fontes;

c) a comunicação de dados seja necessária para a execução de contrato ou contratos em que o titular dos dados seja parte ou de diligências prévias à formação do contrato ou declaração negocial efectuadas a seu pedido;

d) a comunicação de dados seja necessária para o cumprimento de obrigação legal a que o responsável pelo tratamento que transmite os dados ou o destinatário estejam sujeitos, como sucede se a comunicação tiver por finalidade o exercício das actividades atribuídas aos Tribunais (incluindo o Tribunal de Contas), ao Ministério Público, ao Provedor de Justiça e aos órgãos de defesa e segurança do Estado Angolano;

e) se verifiquem as condições que legitimam o tratamento de dados pessoais sem consentimento do titular, nos termos dos artigos 12.º a 20.º da presente lei.

3. A comunicação dos dados de crédito e solvabilidade entre instituições bancárias e as autoridades judiciais e de investigação e instrução criminal pode ser feita sem o prévio consentimento do titular dos dados, mediante autorização prévia da Agência de Protecção de Dados.

ARTIGO 23.º

(Comunicação de dados a subcontratado)

1. A comunicação de dados a subcontratado só pode ser efectuada verificadas as seguintes circunstâncias:

a) conclusão de contrato ou outro documento com valor jurídico, reduzido a escrito, cujo conteúdo estabeleça a obrigação de o subcontratado cumprir o disposto na presente lei e actuar de acordo com as instruções do responsável pelo tratamento;

b) notificação à Agência de Protecção de Dados.

2. Salvo se o responsável pelo tratamento instruir o subcontratado em contrário, este fica sujeito às seguintes obrigações:

a) obrigação de não comunicar os dados pessoais a outros destinatários;

b) obrigação de cumprir as medidas e níveis de segurança estabelecidas na presente lei;

c) obrigação de destruir os dados pessoais ou de devolvê-los ao responsável pelo tratamento finda a relação contratual.

3. O subcontratado não pode tratar dados pessoais para finalidades próprias, nem os pode comunicar a outros destinatários em desrespeito do número anterior, sob pena de, caso o faça, ser considerado responsável pelo tratamento dos mesmos.

4. O disposto neste artigo é aplicável a qualquer operação de tratamento de dados pessoais efectuada por subcontratado.

ARTIGO 24.º

(Interconexão de dados pessoais)

1. A interconexão de dados pessoais só pode ser efectuada mediante autorização da Agência de Protecção de Dados, salvo se estiver prevista em disposição legal.

2. A Agência de Protecção de Dados só autoriza a interconexão de dados se a interconexão:

a) for adequada à prossecução das finalidades legais ou estatutárias e dos interesses legítimos dos responsáveis pelo tratamento;

b) não implicar discriminação, lesão ou diminuição dos direitos, liberdades e garantias fundamentais dos titulares dos dados; e

c) estiver rodeada de adequadas medidas e níveis de segurança.

SECÇÃO IV

Direitos dos Titulares dos Dados

ARTIGO 25.º

(Direito de informação)

1. Sem prejuízo do disposto em outros artigos da presente lei, o responsável pelo tratamento deve disponibilizar aos titulares dos dados pelo menos a seguinte informação:

a) a identidade e endereço do responsável pelo tratamento;

b) as finalidades do tratamento e a criação de um ficheiro com a referida finalidade;
c) os destinatários ou categorias de destinatários dos dados;
d) o carácter obrigatório ou facultativo da resposta, bem como as possíveis consequências de não responder;
e) a existência e condições do direito de acesso e de rectificação, actualização, eliminação e oposição;
f) as consequências da recolha dos dados sem o consentimento do titular ou, em caso de incapacidade deste, pelo seu representante legal;
g) outras informações necessárias para garantir o tratamento lícito de tais dados pessoais.

2. Quando os dados pessoais sejam recolhidos directamente do titular dos dados, a informação deve ser prestada no momento da recolha, excepto se já tiver sido prestada em momento prévio.

3. Caso os dados pessoais não sejam recolhidos directamente do titular dos dados, o responsável pelo tratamento deve prestar-lhe a informação referida no momento do registo dos dados ou o mais tardar no prazo de trinta dias após a sua recolha, salvo se dele já for conhecida.

4. A informação deve ser prestada de maneira clara, precisa e objectiva em particular quando tenha como destinatários menores e pessoas com necessidades especiais.

5. A obrigação de informação pode ser dispensada mediante disposição legal ou deliberação da Agência de Protecção de Dados, nos seguintes casos:

a) por motivos de segurança do Estado e prevenção ou investigação criminal;
b) quando a prestação de informação ao titular dos dados se revelar impossível ou implicar esforços desproporcionados, nomeadamente nos casos de tratamento de dados com finalidades estatísticas, históricas ou de investigação científica; ou
c) quando a lei determinar expressamente o registo dos dados ou a sua divulgação.

6. A obrigação de informação, nos termos do número anterior, não se aplica ao tratamento de dados efectuado para fins exclusivamente jornalísticos ou de expressão artística ou literária.

7. No caso de recolha de dados em redes abertas, considera-se prestado o direito de informação através da publicação e disponibilização de políticas de privacidade que sejam de fácil acesso e incluam:

a) as informações descritas no n.º 1 do presente artigo;
b) a informação de que os seus dados pessoais podem circular na rede sem condições de segurança, correndo o risco de serem vistos e utilizados por terceiros não autorizados.

ARTIGO 26.º
(Direito de acesso)

1. O titular dos dados tem o direito de obter do responsável pelo tratamento, livremente, sem restrições, demoras ou custos excessivos, informação sobre se são ou não tratados dados que lhe digam respeito, as finalidades desse tratamento, as categorias de dados sobre que incide e os destinatários ou categorias de destinatários a quem são comunicados os dados.

2. O responsável pelo tratamento deve ainda comunicar ao titular os dados específicos objecto de tratamento, bem como quaisquer informações disponíveis sobre a origem desses dados.

3. Sem prejuízo do disposto em legislação específica, no tratamento de dados pessoais relativos à segurança do Estado, à prevenção ou investigação criminal e ao segredo de justiça, o direito de acesso é exercido através da Agência de Protecção de Dados.

4. No tratamento de dados pessoais efectuado para fins exclusivamente jornalísticos, o direito de acesso é exercido pela Agência de Protecção de Dados com salvaguarda das normas constitucionais aplicáveis, designadamente as que garantem a liberdade de expressão e a liberdade de imprensa.

5. Nos casos previstos nos n.ºs 3 e 4, se o acesso aos dados pelo seu titular puder prejudicar a segurança do Estado, a prevenção ou a investigação criminal, o segredo de justiça ou ainda a liberdade de expressão e a liberdade de imprensa, a Agência de Protecção de Dados limita-se a informar o titular dos dados das diligências efectuadas.

6. A lei pode restringir o direito de acesso verificadas as seguintes circunstâncias:

a) os dados não serem utilizados para tomar medidas ou decisões relativamente a pessoas determinadas, mas exclusivamente para fins de investiga-

ção científica ou conservados sob forma de dados pessoais durante um período que não exceda o necessário à finalidade exclusiva de elaborar estatísticas;

b) não existir qualquer perigo de violação dos direitos, liberdades e garantias fundamentais do titular dos dados pessoais, designadamente do direito à reserva de intimidade da vida privada.

7. O direito de acesso do titular dos dados à informação sobre os dados de saúde e vida sexual, incluindo os dados genéticos, é exercido por intermédio de médico escolhido pelo titular dos dados ou de seu representante legítimo.

ARTIGO 27.º

(Direito de oposição)

O titular dos dados tem o direito de:

a) salvo disposição legal em contrário, e pelo menos nas situações referidas nas alíneas *d*) e *e*) do n.º 2 do artigo 12.º, se opor em qualquer altura a que os dados que lhe digam respeito sejam objecto de tratamento quando existam razões ponderosas e legítimas relacionadas com a sua situação particular, devendo neste caso o responsável excluir do tratamento tais dados;

b) se opor ao tratamento dos seus dados em outras circunstâncias previstas na presente lei e em outra legislação específica.

ARTIGO 28.º

(Direito de rectificação, actualização e eliminação)

1. É assegurado ao titular dos dados pessoais os direitos de rectificação, actualização ou eliminação dos seus dados pessoais cujo tratamento não cumpra o disposto na presente lei, nomeadamente devido ao carácter incompleto ou inexacto desses dados.

2. O responsável pelo tratamento é obrigado, nos termos da presente lei e legislação especial, a assegurar o direito de rectificação, actualização e eliminação de dados num período de sessenta dias úteis.

3. Se os dados objecto de rectificação, actualização ou eliminação tiverem sido previamente comunicados a destinatário, o responsável pelo tratamento fica obrigado a notificar a este tal rectificação, actualização ou eliminação, salvo se isso for comprovadamente impossível, devendo o destinatário agir em conformidade.

4. No caso previsto no número anterior, o destinatário que tratar os dados para os seus próprios fins ou para fins de um terceiro pode não proceder à eliminação dos dados, devendo neste caso tal destinatário informar o titular dos dados desta situação e confirmar se este pretende também rectificar, actualizar ou eliminar os seus dados dos ficheiros respectivos.

5. O responsável pelo tratamento deve, contudo, bloquear e/ou conservar os dados pessoais nos seguintes casos:

a) disposição legal ou ordem de autoridade competente que obrigue o responsável pelo tratamento a bloquear e/ou conservar os dados por um determinado período de tempo;

b) se o bloqueamento e/ou conservação dos dados for necessário à prossecução de um interesse legítimo do responsável pelo tratamento, designadamente para o exercício de um direito ou para o cumprimento de obrigações legais;

c) se os dados estiverem a ser utilizados para efeitos de investigação criminal;

d) se os dados se tratarem de dados relativos ao crédito e à solvabilidade, enquanto a situação creditícia do titular não estiver regularizada.

ARTIGO 29.º

(Decisões individuais automatizadas)

1. Qualquer pessoa tem o direito de não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afecte de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspectos da sua personalidade, designadamente, a sua capacidade profissional, o seu crédito, a confiança de que é merecedora ou o seu comportamento.

2. Sem prejuízo do cumprimento das restantes disposições da presente lei, uma pessoa pode ficar sujeita a uma decisão tomada nos termos do número anterior, desde que tal ocorra no âmbito da celebração ou da execução de um contrato e sob condição de o seu pedido de celebração ou execução do contrato ter sido satisfeito, ou de existirem medidas adequadas que garantam a defesa dos seus interesses legítimos, designadamente o seu direito de representação e expressão.

3. Pode ainda ser permitida a tomada de uma decisão, nos termos do n.º 1 deste artigo, quando a Agência de Protecção de Dados o autorize, definindo medidas de garantia da defesa dos interesses legítimos do titular dos dados.

ANEXO 5

Quinta-feira, 16 de Fevereiro de 2017 — I Série – N.º 27

DIÁRIO DA REPÚBLICA

ÓRGÃO OFICIAL DA REPÚBLICA DE ANGOLA

Preço deste número - Kz: 220,00

Toda a correspondência, quer oficial, quer relativa a anúncio e assinaturas do «Diário da República», deve ser dirigida à Imprensa Nacional - E.P., em Luanda, Rua Henrique de Carvalho n.º 2, Cidade Alta, Caixa Postal 1306, www.imprensanacional.gov.ao - End. teleg.: «Imprensa».

ASSINATURA

	Ano
As três séries	Kz: 611 799.50
A 1.ª série	Kz: 361 270.00
A 2.ª série	Kz: 189 150.00
A 3.ª série	Kz: 150 111.00

O preço de cada linha publicada nos Diários da República 1.ª e 2.ª série é de Kz: 75.00 e para a 3.ª série Kz: 95.00, acrescido do respectivo imposto do selo, dependendo a publicação da 3.ª série de depósito prévio a efectuar na tesouraria da Imprensa Nacional - E. P.

SUMÁRIO

ASSEMBLEIA NACIONAL

Lei n.º 7/17

de 16 de Fevereiro

A presente Lei visa responder, de forma eficaz e eficiente, aos novos desafios da sociedade da informação, à protecção da utilização do espaço cibernético angolano contra os riscos a eles associados e promover a inclusão digital;

Pretende-se, ainda, com a presente Lei, melhorar a oferta da prestação de serviços digitais, o acesso dos cidadãos à informação e ao conhecimento.

A Assembleia Nacional aprova, por mandato do povo, nos termos das disposições combinadas da alínea b) do artigo 161.º, do n.º 2 do artigo 165.º e da alínea d) do n.º 2 do artigo 166.º, todos da Constituição da República de Angola, a seguinte:

LEI DE PROTECÇÃO DAS REDES E SISTEMAS INFORMÁTICOS

CAPÍTULO I
Disposições Gerais

ARTIGO 1.º
(Objecto)

A presente Lei tem como objecto estabelecer o regime jurídico sobre as medidas de protecção das redes e sistemas informáticos.

ARTIGO 2.º
(Âmbito de aplicação)

1. A presente Lei aplica-se ao ciberespaço da República de Angola, contra qualquer acto de ataque, roubo informático, ciber-ataque e incidentes informáticos.

2. Sem prejuízo do disposto do número anterior e do disposto no Código Penal, a presente Lei é aplicável aos factos:

a) Cometidos em território nacional por cidadãos angolanos, estrangeiros ou por pessoa colectiva com domicílio em território angolano, que visem o ciberespaço ou dados informáticos;

b) Praticados fisicamente, total ou parcialmente, em território angolano, ainda que visem sistemas de informação ou dados localizados fora desse território;

c) Praticados no ciberespaço ou dados localizados em território angolano, independentemente do local onde esses factos forem fisicamente praticados;

d) Cometidos por cidadãos estrangeiros não residentes em território angolano, que visem o ciberespaço ou dados informáticos.

3. O disposto na Secção II e III do Capítulo III aplica-se aos operadores de comunicações electrónicas acessíveis ao público e aos prestadores de armazenagem principal, estabelecidos em território nacional.

ARTIGO 3.º
(Regime jurídico subsidiário)

O regime jurídico constante da presente Lei não prejudica:

a) O disposto nas normas constantes dos Tratados e das Convenções Internacionais, continentais e regionais vigentes na ordem jurídica nacional;

b) O disposto em legislação vigente que seja compatível com a presente Lei, nomeadamente:

i) O regime jurídico de protecção de dados pessoais;

ii) O regime jurídico das tecnologias e dos serviços da sociedade da informação;

iii) O regime jurídico das comunicações electrónicas e dos serviços da sociedade da informação.

ARTIGO 4.º
(Definições)

Para efeitos da presente Lei, considera-se:

a) «*Acesso condicional*» — A sujeição do acesso de um serviço a uma assinatura ou qualquer outra forma de autorização prévia individual;

b) «*Assinante*» — A pessoa singular ou colectiva que é parte num contrato com um operador de comunicações electrónicas acessíveis ao público;

c) «*Base de dados*» — As colectâneas de obras, dados ou outros elementos independentes, dispostos de modo sistemático ou metódico e susceptíveis de acesso individual por meios electrónicos ou outros;

d) «*CERT*» — Centro de Estudos, Respostas e Tratamento de incidentes informáticos;

e) «*Ciber-Ataque*» — O ataque efectuado geralmente através da *Internet*, no qual são violados sistemas informáticos, com o objectivo de espiar, provocar danos, roubar dados;

f) «*Ciberespaço*» — O conjunto dos sistemas tecnológicos e infra-estruturas de redes telemáticas, bem como do conjunto de informações e serviços da *Internet*;

g) «*Cibercrime*» — O crime cometido com o recurso aos sistemas electrónicos e as novas tecnologias de informação e comunicação;

h) «*Cibersegurança*» — A segurança relacionada com o ciberespaço;

i) «*Código de acesso*» — Dado ou senha que permite aceder, no todo ou em parte e sob forma inteligível, à um sistema de informação;

j) «*Código de identificação do utilizador (User ID)*» — O código único atribuído às pessoas, quando estas se tornam assinantes ou se registam num serviço de acesso a *Internet*, ou num serviço de comunicação pela *Internet*;

k) «*Conteúdos discriminatórios*» — Qualquer palavra, imagem ou outro que defenda, promova ou incite ao ódio ou a actos de violência contra uma pessoa ou grupo de pessoas por causa da sua raça, origem étnica, cor, nacionalidade, religião ou orientação sexual, com o propósito de os discriminar;

l) «*Dados*» — Qualquer representação de factos, vídeos ou imagens, informações ou conceitos, incluindo de programas de computador, que são armazenados, transmitidos ou processados num sistema de informação;

m) «*Dados de base pessoais*» — Os dados que permitem identificar uma pessoa, como seja o nome, idade, morada, telefone e endereço de correio electrónico;

n) «*Dados de localização*» — Quaisquer dados tratados num sistema de informação que indiquem a posição geográfica do equipamento terminal ou de um utilizador de um serviço prestado através de um sistema de informação;

o) «*Dados de tráfego*» — Qualquer dado tratado para efeitos do envio de uma comunicação, através de um sistema de informação ou para efeitos de facturação daquela, incluindo os dados que indicam a origem, destino, trajecto, hora, data, tamanho e duração da comunicação, ou o tipo de serviço subjacente;

p) «*Dados informáticos*» — Quaisquer dados susceptíveis de processamento por um sistema informático;

q) «*Dispositivo*» — Qualquer equipamento, material electromagnético, acústico, mecânico, técnico ou outros ou programa de computador;

r) «*DSL (Digital Subscriber Line)*» — A tecnologia que permite aproveitar o conjunto de pares de cabo de cobre para fins de serviços de *Internet* de banda larga;

s) «*Endereço do Protocolo IP*» — O conjunto de números que permitem a identificação e a comunicação consistente entre equipamentos (normalmente computadores) de uma rede privada ou pública, mediante uma plataforma de *Internet*;

t) «*Identificador de Célula (Cell ID)*» — A identificação da célula de origem e de destino de uma chamada telefónica numa rede móvel;

u) «*IMEI (International Mobile Equipmentidentity)*» — O código pré-gravado nos telefones móveis da tecnologia GSM, que permite a identificação do equipamento ou do terminal a nível internacional, ao ser transmitido ou ao interligar-se a uma rede de comunicações electrónicas acessíveis ao público. Caso a tecnologia usada não seja GSM

considera-se o código equivalente para a tecnologia em questão;

v) «*IMSI (International Mobile Subcriberidentity)*» — O código único de identificação para cada aparelho terminal de telefonia móvel cuja integração no cartão SIM do telemóvel, permite a sua identificação através das redes da tecnologia GSM e UMTS. Caso a tecnologia usada não seja GSM e UMTS considera-se o código equivalente para a tecnologia em questão;

w) «*Incidentes informáticos*» — Qualquer evento real ou suspeito relacionado com a segurança de sistema informático ou rede;

x) «*Intercepção de Comunicação*» — O acto destinado a captar dados contidos ou transmitidos através de um sistema de informação mediante o recurso a dispositivos;

y) «*Operadores de comunicações electrónicas*» — Os organismos, as pessoas colectivas de direito público, as pessoas singulares ou colectivas de direito privado ou misto, que oferecem redes ou serviços de comunicações electrónicas;

z) «*Operadores de comunicações electrónicas acessíveis ao público*» — São os operadores de redes de comunicações electrónicas públicas e os operadores de serviços de comunicações electrónicas públicos, conforme estes sejam definidos na legislação relevante;

aa) «*Prestador de serviço*» — Qualquer pessoa, singular ou colectiva, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema de informação, bem como qualquer outra entidade que trate ou armazene dados em nome e por conta daquela ou dos respectivos utilizadores, incluindo, mas não se limitando, a operadores de comunicações electrónicas e prestadores de serviços da sociedade da informação;

bb) «*Programa de computador*» — O conjunto de instruções (*software*) usado directa ou indirectamente num computador, tendo em vista a obtenção de determinado resultado, incluindo o material de concepção;

cc) «*Rede*» — O grupo de sistemas de informação interligados entre si que permite o envio e a recepção de dados;

dd) «*Rede do ciberespaço*» — Os sistemas de transmissão e, se for o caso, os equipamentos de comutação ou encaminhamento e os demais recursos que permitem o envio de sinais por cabo, meios radioeléctricos, meios ópticos, ou por outros meios electromagnéticos, incluindo as redes de satélites, as redes terrestres fixas (com comutação de circuitos ou de pacotes, incluindo a *Internet*) e móveis, os sistemas de cabos de electricidade, na medida em que sejam utilizados para a transmissão de sinais, as redes utilizadas para a radiodifusão sonora e televisiva e as redes de televisão por cabo, independentemente do tipo de informação transmitida;

ee) «*Roubo informático*» — Qualquer apropriação indevida de uma rede, sistema informático, bases de dados, equipamento informático, programa informático, usando a violência, ameaça, acesso ilegítimo com vista a estruturação incorrecta de programa ou sistema informático;

ff) «*Serviço da sociedade da informação*» — O Serviço prestado à distância por via electrónica, no âmbito de uma actividade económica na sequência de pedido individual do destinatário, considerando-se, para efeitos da presente definição:

i. «*Serviço*» — A disponibilização de conteúdos, bens (materiais e imateriais) e serviços, independentemente de a sua entrega ou prestação ser efectuada por via electrónica;

ii. «*À distância*» — Sem que as partes estejam simultaneamente presentes;

iii. «*Por via electrónica*» — Enviado da origem e recebido no destino através de meios electrónicos de processamento e de armazenamento de dados, incluindo a via informática, o cabo, rádio, meios ópticos e meios electromagnéticos, excluindo o telefone, telecópia, telex e teletexto televisivo;

iv. «*Pedido individual do destinatário*» — A solicitação do destinatário para que lhe seja prestado um serviço da sociedade da informação, incluindo o mero acesso ao sítio/página do prestador do serviço da sociedade da informação;

v. Não são serviços da sociedade da informação:

i) Serviços de radiodifusão televisiva e sonora;

ii) Distribuição automática de notas e bilhetes;

iii) Acesso às redes rodoviárias, parques de estacionamento, etc., mediante pagamento, mesmo que existam dispositivos electrónicos à entrada e ou à saída para controlar o acesso ou garantir o correcto pagamento.

gg) «*Serviço protegido*» — Qualquer serviço da sociedade da informação, com acesso condicional;

hh) «*Sistema de informação*» — Qualquer dispositivo ou conjunto de dispositivos, bem como a rede que suporta a comunicação entre eles, que, de forma separada ou conjunta, armazenam, tratam, transmitem, recebem ou recuperam dados;

3. A destruição dos dados previstos no n.º 1 do presente artigo, não prejudica a sua conservação para outros fins, desde que cumpridos os requisitos constantes da lei aplicável.

SECÇÃO V
Preservação da Soberania, Segurança do Estado e Ordem Pública

ARTIGO 39.º
(Sistema de Intercepção de dados)

Os operadores de comunicações electrónicas acessíveis ao público devem assegurar o acesso aos órgãos de inteligência e de segurança do Estado mediante autorização prévia do Magistrado competente, para proceder a intercepção de comunicações, nos termos do artigo 212.º da Constituição da República de Angola.

CAPÍTULO IV
Equipa de Monitorização e Respostas aos Incidentes Informáticos

ARTIGO 40.º
(Organização e funcionamento)

A organização e funcionamento da Equipa de Monitorização e Respostas aos Incidentes Informáticos são estabelecidos por diploma próprio.

ARTIGO 41.º
(Cooperação institucional)

A Equipa de Monitorização e Respostas aos Incidentes Informáticos deve estabelecer relações de cooperação institucional com organismos públicos e privados e outras congéneres na promoção da protecção e segurança do ciberespaço nacional.

CAPÍTULO V
Regime Sancionatório

ARTIGO 42.º
(Contravenções e multas)

1. Sem prejuízo de outras sanções que se mostrem aplicáveis, constitui contravenção punível com multa, a prática dos seguintes actos:

a) O incumprimento dos requisitos previstos nos artigos 12.º, 13.º, 14.º, 15.º e 18.º da presente Lei é aplicável uma multa que varia de Kz: 7.000.000,00 (sete milhões de Kwanzas) a Kz: 150.000.000,00, (cento e cinquenta milhões de Kwanzas);

b) O incumprimento dos requisitos previstos nos artigos 16.º, 17.º, 19.º, 21.º e 23.º da presente Lei é aplicável uma multa que varia de Kz: 7.000.000,00 (sete milhões de Kwanzas) a Kz: 150.000.000,00 (cento e cinquenta milhões de kwanzas);

c) A não conservação das categorias dos dados previstos nos artigos 29.º, 30.º e 31.º da presente Lei é aplicável uma multa que varia de Kz: 7.000.000,00 (sete milhões de Kwanzas) a Kz : 150.000.000,00 (cento e cinquenta milhões de kwanzas);

d) A não conservação das categorias dos dados previstos nos artigos 32.º, 33.º e 34.º da presente Lei é aplicável uma multa que varia de Kz: 3.000.000,00 (três milhões de kwanzas) a Kz: 75.000.000,00 (setenta e cinco milhões de Kwanzas);

e) A não conservação das categorias dos dados previstos no n.º 1 do artigo 37.º é aplicável uma multa que varia de Kz: 1.000.000,00 (um milhão de Kwanzas) a Kz: 3.000.000,00 (três milhões de Kwanzas);

2. É aplicável uma Multa que varia de Kz: 5.000.000,00 (cinco milhões Kwanzas) a Kz: 200.000.000,00 (duzentos milhões de Kwanzas) nos seguintes casos:

a) O incumprimento do disposto no artigo 35.º da presente Lei;

b) Falta de transmissão dos dados às autoridades judiciais competentes, quando autorizada nos termos do n.º 1 do artigo 36.º da presente Lei;

c) O incumprimento das medidas de destruição dos dados, nos termos do artigo 38.º da presente Lei.

3. Tratando-se de pessoas colectivas, as contravenções previstas no número anterior são agravadas ao dobro dos respectivos limites.

4. A determinação da medida da multa é feita em função da ilicitude concreta do facto, da culpa do agente e dos benefícios obtidos com a prática da contravenção e das exigências de prevenção.

5. Na determinação da ilicitude concreta do facto e da culpa deve atender-se, entre outras, às seguintes circunstâncias:

a) Ao perigo ou ao dano causados;

b) Ao carácter ocasional ou reiterado da infracção;

c) A existência de actos de ocultação tendentes a dificultar a descoberta da infracção;

d) A existência de actos praticados pelo agente, destinados a reparar por sua livre iniciativa, os danos ou obviar os perigos causados pela infracção;

e) A intenção do agente de obter, para si ou para outrem, um benefício ilegítimo ou de causar danos.

6. Na determinação da multa aplicável são ainda ponderadas a situação económica do infractor e o volume de negócios consolidado no ano civil anterior.

7. Se o mesmo facto constituir, simultaneamente, crime e contravenção, o agente é punido sempre a título de crime, nos termos previstos da legislação Penal.

8. As sanções aplicadas às contravenções em concurso são sempre cumuladas materialmente.

ARTIGO 43.º
(Aplicação das multas)

1. Compete à Agência de Protecção de Dados Pessoais a instrução dos processos de contravenção.

2. A aplicação das multas previstas na presente Lei compete ao Presidente da Agência de Protecção de Dados Pessoais, sob prévia deliberação da Agência.

ANEXO 6

Segunda-feira, 15 de Outubro de 2012 I Série – N.º 197

DIÁRIO DA REPÚBLICA

ÓRGÃO OFICIAL DA REPÚBLICA DE ANGOLA

Preço deste número - Kz: 280,00

Toda a correspondência, quer oficial, quer relativa a anúncio e assinaturas do «Diário da República», deve ser dirigida à Imprensa Nacional - E.P., em Luanda, Rua Henriques de Carvalho n.º 2, Cidade Alta, Caixa Postal 1306, www.imprensanacional.gov.ao - End. teleg.: «Imprensa».

ASSINATURA	Ano
As três séries	Kz: 440 375.00
A 1.ª série	Kz: 260 250.00
A 2.ª série	Kz: 135 850.00
A 3.ª série	Kz: 105 700.00

O preço de cada linha publicada nos Diários da República 1.ª e 2.ª série é de Kz: 75.00 e para a 3.ª série Kz: 95.00, acrescido do respectivo imposto do selo, dependendo a publicação da 3.ª série de depósito prévio a efectuar na tesouraria da Imprensa Nacional - E. P.

IMPRENSA NACIONAL - E. P.
Rua Henrique de Carvalho n.º 2
E-mail-imprenac@hotmail.com
Caixa Postal N.º 1306

CIRCULAR

Excelentíssimos Senhores:

Havendo necessidade de se evitarem os inconvenientes que resultam para os nossos serviços do facto das respectivas assinaturas no *Diário da República* não serem feitas com a devida oportunidade.

Para que não haja interrupção no fornecimento do *Diário da República* aos estimados clientes, temos a honra de informá-los que estão abertas a partir desta data até 15 de Fevereiro de 2013, as respectivas assinaturas para o ano 2013 pelo que deverão providenciar a regularização dos seus pagamentos junto dos nossos serviços.

1. Estando de momento os preços das assinaturas do *Diário da República* em fase de revisão para um possível reajustamento, e urgindo de momento a necessidade por parte dos nossos assinantes de confirmarem o fornecimento do *Diário da República* para o ano 2013, passam a título provisório a vigorar em território nacional os preços em vigor, acrescido do Imposto de Consumo a taxa de 2% (dois porcentos):

As 3 séries ..... Kz: 463 125,00
1.ª série ..... Kz: 273 700,00
2.ª série ..... Kz: 142 870,00
3.ª série ..... Kz: 111 160,00

2. Tão logo seja publicado o preço definitivo em *Diário da República* ou cobrança pela Imprensa Nacional – E.P. mediante correspondência, os assinantes terão o prazo de 45 (quarenta e cinco) dias para liquidar a diferença apurada, para assegurar a continuidade do fornecimento durante o período em referência.

3. As assinaturas serão feitas apenas em regime anual.

4. Aos preços mencionados no n.º 1 acrescer-se-á um valor adicional para portes de correio por via normal das três séries, para todo o ano, no valor de Kz: 95 975.00 que poderá sofrer eventuais alterações em função da flutuação das taxas a praticar pela Empresa Nacional de Correios de Angola, E.P., no ano de 2013.

5. Os clientes que optarem pela recepção dos *Diários da República* através do correio deverão indicar o seu endereço completo, incluindo a Caixa Postal, a fim de se evitarem atrasos na sua entrega, devolução ou extravio.

Observações:

a) Estes preços poderão ser alterados se houver uma desvalorização da moeda nacional, numa proporção superior à base que determinou o seu cálculo ou outros factores que afectem consideravelmente a nossa estrutura de custos;

b) As assinaturas que forem feitas depois de 15 de Fevereiro de 2013 sofrerão um acréscimo aos preços em vigor de uma taxa correspondente a 15%;

c) Aos organismos do Estado que não regularizem os seus pagamentos das dívidas até 15 de Dezembro do ano em curso não lhes serão concedidas a crédito as assinaturas do Diário da República para o ano de 2013.

SUMÁRIO

Presidente da República

e) Secretaria para Assuntos Sociais;
f) Secretaria para Assuntos Regionais e Locais;
g) Secretaria para Assuntos de Comunicação Institucional e Imprensa.

2. As Secretarias da Casa Civil do Presidente da República são dirigidas por Secretários de Estado, que exercem as funções de Secretários.

3. Integram, ainda, a Casa Civil do Presidente da República, como órgãos de assistência ao Presidente da República:

a) Director do Gabinete do Presidente da República;
b) Director Adjunto do Gabinete do Presidente da República;
c) Director do Cerimonial do Presidente da República;
d) Director Adjunto do Cerimonial do Presidente da República;
e) Consultores do Presidente da República;
f) Secretários Particulares do Presidente da República.

4. Junto da Casa Civil do Presidente da República funcionam também:

a) Gabinete de Quadros;
b) Gabinete da Primeira Dama.

5. O Gabinete de Quadros do Presidente da República é dirigido por um Director, com a categoria de Ministro.

6. O Gabinete do Presidente da República é dirigido por um Director, com a categoria de Secretário de Estado e coadjuvado por um Adjunto com a categoria de Vice-Ministro.

7. O Cerimonial do Presidente da República é dirigido por um Director, com a categoria de Secretário de Estado e coadjuvado por um Adjunto com a categoria de Vice-Ministro.

ARTIGO 14.º
(Organização e funcionamento)

A organização e funcionamento da Casa Civil do Presidente da República são fixados por Decreto Presidencial.

SECÇÃO III
Casa de Segurança do Presidente da República

ARTIGO 15.º
(Função)

1. A Casa de Segurança do Presidente da República é o órgão com a finalidade de prestar assistência, assessoria e apoio técnico directo e imediato ao Presidente da República e Chefe de Estado no desempenho das suas funções, especialmente em assuntos de segurança nacional e na garantia de segurança e defesa presidencial.

2. A Casa de Segurança do Presidente da República é dirigida pelo Ministro de Estado e Chefe da Casa de Segurança.

ARTIGO 16.º
(Estrutura)

1. A Casa de Segurança do Presidente da República tem a seguinte estrutura:

a) Secretária Executiva;
b) Secretaria para Assuntos de Defesa e Forças Armadas;
c) Secretaria para Assuntos de Interior e Polícia Nacional;
d) Secretaria para Assuntos dos Órgãos de inteligência e de Segurança de Estado;
e) Secretaria para a Logística e Infra-Estruturas;
f) Secretaria para os Assuntos de Telecomunicações e de Informática;
g) Secretaria para o Pessoal e Quadros;
h) Secretaria Geral da Casa de Segurança.

2. As Secretarias da Casa de Segurança do Presidente da República são dirigidas por Secretários.

3. Integram, ainda, a Casa de Segurança do Presidente da República, como órgãos de assistência e apoio ao Presidente da República.

a) Gabinete de Estudos de Segurança;
b) Gabinete de Acção Psicológica e de Informação;
c) Gabinete de Voo Presidencial;
d) Serviços de Saúde da Casa de Segurança;
e) Centro de Direcção, Telecomunicações e Informática do Presidente da República e Comandante-Em-Chefe.

4. Junto da Casa de Segurança do Presidente da República funcionam como órgãos de assistência e apoio técnico ao Presidente da República e Comandante-Em-Chefe, as seguintes estruturas:

a) Unidade de Segurança Presidencial;
b) Unidade de Guarda Presidencial;
c) Clínica Multiperfil;
d) Gabinete de Obras Especiais.

ARTIGO 17.º
(Organização e funcionamento)

A organização e funcionamento da Casa de Segurança do Presidente da República são fixados por Decreto Presidencial.

SECÇÃO IV
Secretaria Geral do Presidente da República

ARTIGO 18.º
(Função)

1. A Secretaria Geral do Presidente da República é o órgão de apoio técnico ao Presidente da República, incumbido de organizar, coordenar e controlar toda a actividade administrativa financeira logística e de assistência técnica necessária ao funcionamento do Presidente da República e de todos os órgãos sob sua coordenação.

2. A Secretaria Geral do Presidente da República é dirigida, por um Ministro, que exerce as funções de Secretário Geral.

ARTIGO 19.º
(Estrutura)

1. A Secretaria Geral do Presidente da República tem a seguinte estrutura:

a) Direcção de Administração e Finanças;
b) Direcção de Manutenção e Obras;
c) Direcção de Transportes.

2. As Direcções da Secretaria Geral do Presidente da República são dirigidas por Directores.

3. Integram, ainda, a Secretaria Geral como órgãos de apoio técnico ao Presidente da República:

a) Centro de Documentação e Informação;

b) Chancelaria das Ordens e Condecorações.

4. Junto da Secretaria Geral funciona também o Administrador do Palácio.

ARTIGO 20.º
(Organização e funcionamento)

A organização e funcionamento da Secretaria Geral do Presidente da República são fixados por Decreto Presidencial.

CAPÍTULO V
Órgãos Colegiais de Consulta do Presidente da República e Chefe de Estado

SECÇÃO I
Conselho da República

ARTIGO 21.º
(Função)

O Conselho da República é o órgão Colegial de consulta do Presidente da República.

ARTIGO 22.º
(Atribuições)

Ao Conselho da República incumbe o seguinte:

a) Pronunciar-se sobre a Declaração da Guerra e a feitura da paz;

b) Pronunciar-se sobre o estado de sítio e o seu retorno a normalidade;

c) Pronunciar-se sobre o estado de emergência e o seu retorno a normalidade;

d) Apreciar o Regimento do Conselho da República;

e) Aconselhar o Presidente da República no exercício das suas funções e competências sempre que este lhe solicitar.

ARTIGO 23.º
(Composição)

1. O Conselho da República é presidido pelo Presidente da República e é composto pelos seguintes membros:

a) Vice-Presidente da República;

b) Presidente da Assembleia Nacional;

c) Presidente do Tribunal Constitucional;

d) Procurador Geral da República;

e) Antigos Presidentes da República que não tenham sido destituídos;

f) Presidentes dos Partidos Políticos e das Coligações de Partidos Políticos representados na Assembleia Nacional;

g) Dez (10) cidadãos designados pelo Presidente da República, pelo período correspondente a duração do seu mandato;

h) O Presidente da República pode convidar outras entidades para assistirem as reuniões do Conselho da República.

ARTIGO 24.º
(Organização e funcionamento)

1. O Conselho da República rege-se por um Regimento aprovado por Decreto Presidencial.

2. O Conselho da República é apoiado técnica e administrativamente por um secretariado dirigido pelo Ministro de Estado e Chefe da Casa Civil.

3. As reuniões do Conselho da República não são públicas.

SECÇÃO II
Conselho de Segurança Nacional

ARTIGO 25.º
(Função)

O Conselho de Segurança Nacional é o órgão de consulta do Presidente da República para assuntos relativos à condução da política e estratégia da segurança nacional, bem como a organização, funcionamento e disciplina das Forças Armadas, da Polícia Nacional e demais Órgãos da Protecção Interior e dos Órgãos de Inteligência e de Segurança de Estado, nos termos da Constituição.

ARTIGO 26.º
(Composição)

1. O Conselho de Segurança Nacional é presidido pelo Presidente da República e composto pelos seguintes membros:

a) Vice-Presidente da República;

b) Presidente da Assembleia Nacional;

c) Presidente do Tribunal Constitucional;

d) Presidente do Tribunal Supremo;

e) Procurador Geral da República;

f) Ministro de Estado e Chefe da Casa Civil do Presidente da República;

g) Ministro de Estado e Chefe da Casa de Segurança do Presidente da República;

h) Ministro da Defesa Nacional;

i) Ministro do Interior;

j) Ministro das Relações Exteriores;

k) Ministro da Justiça e dos Direitos Humanos;

l) Ministro das Finanças;

m) Chefe do Estado Maior General das Forcas Armadas Angolanas;

n) Comandante Geral da Polícia Nacional;

o) Chefe do Serviço de Inteligência e de Segurança de Estado;

p) Chefe do Serviço de Inteligência Militar;

q) Director Geral do Serviço de Inteligência Externa.

2. O Presidente da República pode convidar outras entidades para assistirem as reuniões do Conselho de Segurança Nacional.

3. As reuniões do Conselho de Segurança Nacional não são públicas.

ARTIGO 27.º
(Atribuições)

Ao Conselho de Segurança Nacional incumbe o seguinte:

a) Auxiliar o Presidente da República na formulação e condução da política e estratégia de segurança nacional e dos assuntos político-estratégicos internos e externos relacionados com a segurança nacional;

b) Apreciar a Directiva do Presidente da República e Comandante-Em-Chefe sobre a Segurança Nacional, o Plano de Segurança Nacional e a Programação de Segurança Nacional, incluindo a sua execução;

c) Apreciar questões relativas a organização, preparação e emprego do sistema de segurança nacional;

d) Pronunciar-se acerca da declaração de guerra e da feitura da paz;

e) Pronunciar-se acerca do estado de defesa e do seu retorno a normalidade;

f) Pronunciar-se acerca do estado de sítio e do retorno a normalidade;

g) Pronunciar-se sobre a nomeação e exoneração do Chefe do Estado-Maior General das Forças Armadas Angolanas e do Chefe do Estado-Maior General Adjunto das Forças Armadas Angolanas, bem como dos demais cargos de Comando e Chefia das Forças Armadas Angolanas;

h) Pronunciar-se sobre a promoção e graduação, bem como despromoção e desgraduação dos oficiais generais das Forças Armadas Angolanas;

i) Pronunciar-se sobre a nomeação e exoneração do Comandante Geral da Polícia Nacional e do 2.º Comandante Geral da Polícia Nacional, bem como dos demais cargos de Comando e Chefia da Polícia Nacional;

j) Pronunciar-se sobre a promoção e graduação, bem como da despromoção e desgraduação dos oficiais Comissários da Polícia Nacional;

k) Pronunciar-se sobre a nomeação e exoneração dos titulares, adjuntos e chefes de direcção dos órgãos de inteligência e segurança de Estado;

l) Apreciar as propostas de quadro legal relativo ao sistema de segurança nacional, nomeadamente a legislação pertinente e os documentos conceptuais, doutrinários, regulamentares e operacionais afins;

m) Apreciar o Regimento do Conselho de Segurança Nacional;

n) Apreciar os demais assuntos e questões que lhe sejam submetidos pelo Presidente da República.

ARTIGO 28.º
(Organização e funcionamento)

1. São órgãos do Concelho de Segurança Nacional:

a) A Comissão Técnica do Conselho de Segurança Nacional;

b) O Secretariado do Conselho de Segurança Nacional.

2. O Conselho de Segurança Nacional rege-se por um Regimento aprovado por Decreto Presidencial.

3. As reuniões do Conselho de Segurança Nacional não são públicas.

ARTIGO 29.º
(Comissão Técnica do Conselho de Segurança Nacional)

1. A Comissão Técnica do Conselho de Segurança Nacional é um órgão técnico de apoio directo ao funcionamento do Conselho de Segurança Nacional e de assistência imediata ao Presidente da República e Chefe de Estado, na formulação e condução da política e estratégia da segurança nacional e dos assuntos político-estratégicos, internos e externos que importam a segurança nacional.

2. A organização funcionamento da Comissão Técnica do Conselho de Segurança Nacional é aprovada por Decreto Presidencial.

ARTIGO 30.º
(Secretariado do Conselho de Segurança Nacional)

1. O Secretariado do Conselho de Segurança Nacional é um serviço que assegura a actividade técnica e administrativa do Conselho de Segurança Nacional.

2. O Secretariado do Conselho de Segurança Nacional é dirigido, pelo Ministro de Estado e Chefe da Casa de Segurança do Presidente da República, que exerce as funções de Secretário do Conselho de Segurança.

CAPÍTULO VI
Departamentos Ministeriais Auxiliares do Presidente da República e Titular do Poder Executivo

SECÇÃO I
Estrutura e Atribuições dos Departamentos Ministeriais

ARTIGO 31.º
(Natureza e Direcção)

1. Os Departamentos Ministeriais são órgãos Auxiliares do Presidente da República e Titular do Poder Executivo nas funções de governação e de administração dos seus respectivos sectores, aos quais correspondem áreas específicas de actividade, de acordo com os poderes delegados.

2. Os Departamentos Ministeriais são dirigidos por Ministros de Estado ou Ministros, coadjuvados por Secretários de Estado ou Vice-Ministros.

3. O Presidente da República e Titular do Poder Executivo pode prover Secretários de Estado que funcionam na sua dependência Directa.

CAPÍTULO VIII
Órgãos e Serviços Específicos Auxiliares do Presidente da República e Titular do Poder Executivo

SECÇÃO I
Órgãos de Inteligência e de Segurança de Estado

ARTIGO 49.º
(Serviço de Inteligência e de Segurança de Estado)

1. O Serviço de Inteligência e de Segurança de Estado é o órgão destinado a produzir informações, análises e a realização de medidas e acções de inteligência e de segurança de Estado, visando a garantia da segurança interna do País, a preservação do Estado de Direito Democrático constitucionalmente estabelecido e a protecção da população contra ameaças e vulnerabilidades.

2. O Serviço de Inteligência e de Segurança de Estado é dirigido por um Chefe de Serviço, com a categoria de Secretário de Estado.

3. A organização e funcionamento do Serviço de Inteligência e de Segurança de Estado é fixada por Diploma próprio, aprovado por Decreto Presidencial.

ARTIGO 50.º
(Serviço de Inteligência Externa)

1. O Serviço de Inteligência Externa é o órgão destinado para a produção de informações, análises e para a realização de medidas e acções de inteligência e de segurança de Estado, visando a garantia da segurança externa do País, da preservação do Estado de Direito Democrático constitucionalmente estabelecido, da segurança externa e a protecção da população contra ameaças e vulnerabilidades.

2. O Serviço de Inteligência Externa é dirigido por um Director de Serviço, com a categoria de Secretário de Estado.

3. A organização e funcionamento do Serviço de Inteligência Externa são fixados por Diploma próprio, aprovado por Decreto Presidencial.

ARTIGO 51.º
(Serviço de Inteligência e de Segurança Militar)

1. O Serviço de Inteligência e de Segurança Militar é o órgão destinado a produzir informações, análises e a realização de medidas e acções de inteligência e de segurança de Estado, visando a garantia da segurança militar do País, da preservação do Estado de Direito Democrático constitucionalmente estabelecido e a protecção da população contra ameaças e vulnerabilidades.

2. O Serviço de Inteligência e de Segurança Militar é dirigido por um Chefe de Serviço, com a categoria de Vice-Ministro.

3. A organização e funcionamento do Serviço de Inteligência e de Segurança Militar são fixados por Diploma próprio, aprovado por Decreto Presidencial.

SECÇÃO II
Órgãos de Inspecção do Estado

ARTIGO 52.º
(Natureza)

1. Os Órgãos de Inspecção do Estado são estruturas inspectivas gerais ou sectoriais e de fiscalização para assistir o Presidente da República e Titular do Poder Executivo no exercício das suas funções com vista a assegurar o controlo estratégico da administração directa e indirecta do Estado, bem como das Administrações autónoma e independente, compreendendo o controlo da legalidade, a auditoria e a avaliação, nos termos da lei.

2. São Órgãos de Inspecção do Estado:

a) A Inspecção-Geral da Administração do Estado;

b) Outros serviços de inspecção-geral ou sectorial e de fiscalização integrados em Departamentos Ministeriais ou em instituições públicas com autonomia administrativa, técnica e financeira.

ARTIGO 53.º
(Inspecção-Geral da Administração do Estado)

1. A Inspecção-Geral da Administração do Estado (abreviadamente IGAE) é o órgão auxiliar do Titular do Poder Executivo para a inspecção, auditoria, controlo e fiscalização da actividade dos órgãos, organismos e serviços da administração directa e indirecta do Estado, bem como das Administrações autónoma e independente.

2. A Inspecção-Geral da Administração do Estado é dirigida por um Inspector- Geral do Estado, com a categoria de Ministro.

3. O Inspector-Geral do Estado é coadjuvado por Inspectores-Gerais do Estado Adjuntos, com a categoria de Secretários de Estado.

4. O Inspector-Geral do Estado e respectivos adjuntos são nomeados pelo Presidente da República.

SECÇÃO III
Comissões Especializadas

ARTIGO 54.º
(Natureza)

1. As comissões especializadas são grupos de trabalho de natureza multidisciplinar compostos por órgãos, organismos, serviços ou entidades e que integram a administração directa e central do Estado, para assistir o Presidente da República em determinados assuntos e questões de interesse público, nos termos da lei.

2. Às comissões especializadas são conferidas missões e competências de assessoria, acompanhamento e controle, bem como de superintendência, gestão e execução específicas.

ARTIGO 55.º
(Classificação)

1. As Comissões Especializadas são as seguintes:

a) Comissões Nacionais e Intersectoriais;

b) Comissões Ministeriais.

2. O Presidente da República define por Despacho Presidencial o elenco das Comissões Especializadas, bem como a forma de organização e funcionamento através dos respectivos estatutos ou regulamentos.

ANEXO 7

Segunda-feira, 2 de Dezembro de 2013 — I Série – N.º 231

DIÁRIO DA REPÚBLICA

ÓRGÃO OFICIAL DA REPÚBLICA DE ANGOLA

Preço deste número - Kz: 250,00

Toda a correspondência, quer oficial, quer relativa a anúncio e assinaturas do «Diário da República», deve ser dirigida à Imprensa Nacional - E.P., em Luanda, Rua Henrique de Carvalho, n.º 2, Cidade Alta, Caixa Postal 1306, www.imprensanacional.gov.ao - End. teleg.: «Imprensa»

ASSINATURA

	Ano
As três séries	Kz: 440 375,00
A 1.ª série	Kz: 260 250,00
A 2.ª série	Kz: 135 850,00
A 3.ª série	Kz: 105 700,00

O preço de cada linha publicada nos Diários da República 1.ª e 2.ª série é de Kz: 75,00 e para a 3.ª série Kz: 95,00, acrescido do respectivo imposto do selo, dependendo a publicação da 3.ª série de depósito prévio a efectuar na tesouraria da Imprensa Nacional - E. P.

IMPRENSA NACIONAL - E.P.
Rua Henrique de Carvalho n.º 2
e-mail: imprensanacional@imprensanacional.gov.ao
Caixa Postal N.º 1306

CIRCULAR

Excelentíssimos Senhores,

Temos a honra de convidá-los a visitar a página da *internet* no *site* www.imprensanacional.gov.ao, onde poderá *online* ter acesso, entre outras informações, aos sumários dos conteúdos do *Diário da República* nas três Séries.

Havendo necessidade de se evitarem os inconvenientes que resultam para os nossos serviços do facto de as respectivas assinaturas no *Diário da República* não serem feitas com a devida oportunidade;

Para que não haja interrupção no fornecimento do *Diário da República* aos estimados clientes, temos a honra de informá-los que até 15 de Dezembro de 2013 estarão abertas as respectivas assinaturas para o ano 2014, pelo que deverão providenciar a regularização dos seus pagamentos junto dos nossos serviços.

1. Enquanto não for ajustada a nova tabela de preços a cobrar pelas assinaturas para o fornecimento do *Diário da República* para o ano de 2014, passam, a título provisório, a ser cobrados os preços em vigor, acrescidos do Imposto de Consumo de 2% (dois porcento):

As 3 séries ..... Kz: 470 615,00
1.ª série ..... Kz: 277 900,00
2.ª série ..... Kz: 145 500,00
3.ª série ..... Kz: 115 470,00

2. Tão logo seja publicado o preço definitivo os assinantes terão o prazo de 45 (quarenta e cinco) dias para liquidar a diferença apurada, visando assegurar a continuidade do fornecimento durante o período em referência.

3. As assinaturas serão feitas apenas em regime anual.

4. Aos preços mencionados no n.º 1 acrescer-se-á um valor adicional para portes de correio por via normal das três séries, para todo o ano, no valor de Kz: 95 975,00 que poderá sofrer eventuais alterações em função da flutuação das taxas a praticar pela Empresa Nacional de Correios de Angola - E.P. no ano de 2014.

5. Os clientes que optarem pela recepção dos *Diários da República* através do correio deverão indicar o seu endereço completo, incluindo a Caixa Postal, a fim de se evitarem atrasos na sua entrega, devoluçao ou extravio.

Observações:

a) Estes preços poderão ser alterados se houver uma desvalorização da moeda nacional, numa proporção superior à base que determinou o seu cálculo ou outros factores que afectem consideravelmente a nossa estrutura de custos;

b) As assinaturas que forem feitas depois de 15 de Dezembro de 2013 sofrerão um acréscimo aos preços em vigor de uma taxa correspondente a 15%;

c) Aos organismos do Estado que não regularizem os seus pagamentos das dívidas até 15 de Dezembro do ano em curso não lhes serão concedidas a crédito as assinaturas do Diário da República *para o ano de 2014.*

SUMÁRIO

Presidente da República

Banco Nacional de Angola

Aviso n.º 14/13:

Determina que as instituições financeiras bancárias autorizadas a funcionar, pelo Banco Nacional de Angola, devem ter o seu capital social integralmente realizado em moeda nacional, bem como manter o capital social e os fundos próprios regulamentar (FPR) no valor mínimo de Kz: 2.500.000.000,00. — Revoga a alínea a) do número 1, do artigo 1.º do Aviso n.º 4/07 de 26 de Setembro.

Ministério das Finanças

Despacho n.º 2654/13:

Autoriza a transferência da gestão do Fundo de Pensões Aberto Longa Vida, da AAA Pensões SA, para a BESAACTIF — Sociedade Gestora de Fundos de Pensões SA, em conformidade com o requerimento dos interessados e demais elementos juntos ao processo que se encontram arquivados na Agência Angolana de Regulação e Supervisão de Seguros — ARSEG e aprova a Adenda ao Regulamento de Gestão Fundo de Pensões Aberto Longa Vida.

Despacho n.º 2655/13:

Nomeia Euclides Sebastião Mixinge para o cargo de Chefe do Departamento de Navegação e Controlo do Serviço Regional da Alfândega de Cabinda. — Revoga o Despacho n.º 2201/13, de 10 de Outubro.

Ministério das Telecomunicações e Tecnologias de Informação

Despacho n.º 2656/13:

Indica os membros do Conselho de Administração do Fundo de Apoio ao Desenvolvimento das Comunicações — FADCOM.

PRESIDENTE DA REPÚBLICA

Decreto Presidencial n.º 201/13
de 2 de Dezembro

Considerando que o Decreto Legislativo Presidencial n.º 5/12, de 15 de Outubro, define uma nova organização e funcionamento da Casa de Segurança do Presidente da República, enquanto órgão auxiliar do Presidente da República como Titular do Poder Executivo;

Havendo necessidade de reajustar e actualizar a organização e funcionamento da Casa de Segurança do Presidente da República, e sua respectiva orgânica;

O Presidente da República decreta, nos termos da alínea g) do artigo 120.º e do n.º 3 do artigo 125.º, ambos da Constituição da República de Angola, o seguinte:

ARTIGO 1.º
(Aprovação)

É aprovado o Estatuto Orgânico da Casa de Segurança do Presidente da República, anexo ao presente Diploma e que dele é parte integrante.

ARTIGO 2.º
(Revogação)

É revogado o Decreto Presidencial n.º 181/10, de 20 de Agosto, e toda a legislação que contrarie o disposto no presente Diploma.

ARTIGO 3.º
(Dúvidas e omissões)

As dúvidas e omissões resultantes da interpretação e aplicação do presente Diploma são resolvidas pelo Presidente da República.

ARTIGO 4.º
(Entrada em vigor)

O presente Diploma entra em vigor na data da sua publicação.

Publique-se.

Luanda, aos 6 de Novembro de 2013.

O Presidente da República, José Eduardo dos Santos

ESTATUTO ORGÂNICO DA CASA DE SEGURANÇA DO PRESIDENTE DA REPÚBLICA

CAPÍTULO I
Função e Atribuições

ARTIGO 1.º
(Função)

1. A Casa de Segurança do Presidente da República é o órgão auxiliar do Presidente da República com a finalidade de prestar assistência, assessoria e apoio técnico directo e imediato ao Presidente da República e Chefe de Estado, no desempenho das suas funções, especialmente em assuntos de segurança nacional e na garantia de segurança e defesa presidencial.

2. A Casa de Segurança do Presidente da República é dirigida pelo Ministro de Estado e Chefe da Casa de Segurança.

ARTIGO 2.º
(Natureza e atribuições)

1. A Casa de Segurança tem natureza de Departamento Ministerial.

2. Na prossecução das suas atribuições, compete à Casa de Segurança:

a) Auxiliar o Presidente da República e Comandante-Em-Chefe na formulação, direcção e controlo da execução da política e da estratégia de segurança nacional;

b) Prestar assistência, assessoria e apoio técnico ao Presidente da República em matérias de defesa nacional, de protecção interior, de preservação de segurança de Estado e de preservação complementar de segurança nacional;

c) Assegurar a ligação e articulação institucional com os órgãos e instituições próprias de segurança nacional, bem como com os órgãos e instituições com responsabilidades específicas na execução da segurança nacional;

d) Realizar a segurança e defesa do Presidente da República, assim como da respectiva família, do Palácio Presidencial e demais instalações da Presidência da República, bem como de outras autoridades e instalações quando determinado pelo Presidente da República;

e) Assegurar a Ajudância-de-Campo do Presidente da República em estreita cooperação com a Casa Civil;

f) Assegurar a transportação do Presidente da República e sua respectiva família nas deslocações no interior e exterior do País;

g) Assegurar e ter atenção com a saúde do Presidente da República e respectiva família;

h) Realizar a segurança pessoal do Vice-Presidente da República e dos responsáveis dos órgãos auxiliares do Presidente da República;

i) Realizar as tarefas e actividades permanentes, técnicas e de apoio administrativo necessário ao exercício das atribuições do Secretariado do Conselho de Segurança Nacional;

j) Desempenhar outras tarefas e acções superiormente determinadas.

ARTIGO 3.º
(Princípios básicos)

A Casa de Segurança do Presidente da República, seus órgãos e serviços, bem como os seus servidores públicos, exercem a sua actividade obedecendo os seguintes princípios:

a) O respeito pela Constituição e demais legislação em vigor, a lealdade às instituições e entidades públicas e aos superiores interesses do Estado;

b) A observância da prossecução do interesse público, da probidade administrativa, da integridade e responsabilidade;

c) O respeito pelo regime disciplinar e o cumprimento dos regulamentos.

CAPÍTULO II
Organização em Geral da Casa de Segurança

SECÇÃO I
Direcção da Casa de Segurança

ARTIGO 4.º
(Direcção)

1. A Casa de Segurança do Presidente da República é dirigida pelo Ministro de Estado e Chefe da Casa de Segurança.

2. Nas ausências e impedimentos do Ministro de Estado e Chefe da Casa de Segurança, as funções são desempenhadas por quem for indicado, obtida anuência expressa do Presidente da República.

3. No exercício das suas funções, o Ministro de Estado e Chefe da Casa de Segurança emite Decretos Executivos, Despachos, Instrutivos e Circulares.

ARTIGO 5.º
(Ministro de Estado e Chefe da Casa de Segurança)

1. O Ministro de Estado e Chefe da Casa de Segurança é o órgão singular a quem compete dirigir, superintender, tutelar e orientar a actuação funcional e operacional, a preparação e desenvolvimento da Casa de Segurança.

2. Ao Ministro de Estado e Chefe da Casa de Segurança compete em especial o seguinte:

a) Dirigir, coordenar e fiscalizar a actuação funcional e operacional, a preparação e desenvolvimento da Casa de Segurança, exercendo os poderes de direcção e superintendência, assim como os poderes implícitos deles decorrentes;

b) Auxiliar o Presidente da República e Comandante-Em-Chefe em matéria de segurança nacional;

c) Prestar assistência, assessoria e apoio técnico ao Presidente da República e Comandante-Em-Chefe nos domínios da defesa nacional, de protecção interna e de preservação da segurança do Estado;

d) Coordenar as relações e assegurar a ligação e articulação institucional com os órgãos e instituições próprias de segurança nacional e com os órgãos e instituições com responsabilidades específicas na execução da segurança nacional;

e) Apresentar ao Presidente da República e Comandante-Em-Chefe todos os assuntos de segurança nacional ou correlacionados para a sua apreciação e orientação, bem como promover o respectivo expediente;

f) Coordenar a realização da segurança e defesa do Presidente da República, da respectiva família, do Palácio Presidencial e demais instalações da Presidência da República, bem como de outras autoridades e instalações quando determinado pelo Presidente da República;

g) Representar o Presidente da República sempre que este o determine;

h) Assinar, em nome do Estado, os acordos, protocolos e memorandos de entendimento, bem como os contratos, no âmbito dos domínios de actividade da Casa de Segurança, mediante autorização superior;

i) Assistir às reuniões dos órgãos colegiais auxiliares do Presidente da República;

j) Chefiar o Secretariado do Conselho de Segurança Nacional;

k) Propor a nomeação e exoneração dos Secretários e dos Chefes dos Serviços Especiais e dos Organismos Dependentes da Casa de Segurança;

l) Propor a promoção, a graduação, a despromoção e desgraduação dos oficiais generais em comissão de serviço na Casa de Segurança;

m) Nomear e exonerar os Assistentes e demais responsáveis que exercem diversos cargos de Direcção e Chefia na Casa de Segurança;

n) Praticar os demais actos necessários ao exercício das suas funções, resultante da legislação em vigor e regulamentos, bem como realizar as demais missões, tarefas e actividades incumbidas pelo Presidente da República e Comandante-Em-Chefe.

SECÇÃO II
Órgãos e Serviços da Casa de Segurança

ARTIGO 6.º
(Estrutura)

A Casa de Segurança do Presidente da República tem a seguinte estrutura orgânica:

1. Órgãos Colegiais Consultivos:
   a) Conselho Técnico da Casa de Segurança;
   b) Conselho Superior de Pessoal e Quadros da Casa de Segurança.
2. Serviços de Apoio Instrumental da Casa de Segurança:
   a) Gabinete do Ministro de Estado e Chefe da Casa de Segurança;
   b) Assistentes do Gabinete da Casa de Segurança;
   c) Consultores do Ministro de Estado e Chefe da Casa de Segurança;
   d) Secção de Expediente, Classificação e Arquivo;
   e) Secção de Relações Públicas e Protocolo;
   f) Secção de Interpretação e Tradução.
3. Órgãos Executivos da Casa de Segurança:
   a) Secretaria Executiva da Casa de Segurança;
   b) Secretaria para Assuntos de Defesa e Forças Armadas;
   c) Secretaria para Assuntos de Interior e Polícia Nacional;
   d) Secretaria para Assuntos dos Órgãos de Inteligência e de Segurança de Estado;
   e) Secretaria para a Logística e Infra-estruturas;
   f) Secretaria para Assuntos de Telecomunicações e Informática;
   g) Secretaria para o Pessoal e Quadros;
   h) Secretaria Geral da Casa de Segurança.
4. Integram a Casa de Segurança do Presidente da República, como órgãos especiais de assistência e apoio ao Presidente da República:
   a) Gabinete de Estudos de Segurança;
   b) Gabinete de Acção Psicológica e de Informação;
   c) Gabinete de Voo Presidencial;
   d) Serviços de Saúde da Casa de Segurança;
   e) Centro de Direcção. Telecomunicações e Informática do Presidente da República e Comandante-Em-Chefe.
5. Junto da Casa de Segurança do Presidente da República funcionam como órgãos de assistência e apoio ao Presidente da República e Comandante-Em-Chefe os seguintes organismos dependentes e tutelados:
   a) Unidade de Segurança Presidencial;
   b) Unidade de Guarda Presidencial;
   c) Clínica Multiperfil;
   d) Gabinete de Obras Especiais.

CAPÍTULO III
Organização Específica da Casa de Segurança

SECÇÃO I
Órgãos Colegiais Consultivos da Casa de Segurança

ARTIGO 7.º
(Conselho Técnico da Casa de Segurança)

1. O Conselho Técnico da Casa de Segurança é o órgão consultivo de apoio ao Ministro de Estado e Chefe da Casa de Segurança para as matérias de segurança nacional, bem como a organização, funcionamento e disciplina da Casa de Segurança.

2. Ao Conselho Técnico da Casa de Segurança compete, no âmbito consultivo, emitir parecer sobre:
   a) Matérias de segurança nacional e de interesse geral sempre que lhe for solicitado;
   b) Programar o orçamento da Casa de Segurança, bem como os planos de trabalho e os relatórios de balanço da Casa de Segurança;
   c) Medidas organizativas tendentes ao melhor funcionamento da Casa de Segurança;
   d) Exercer outras funções que lhe sejam submetidas para a apreciação pelo Ministro de Estado e Chefe da Casa de Segurança.

3. O Conselho Técnico da Casa de Segurança é presidido pelo Ministro de Estado e Chefe da Casa de Segurança e integra os seguintes membros:
   a) Secretários da Casa de Segurança;
   b) Chefes dos Órgãos Especiais da Casa de Segurança;
   c) Chefes dos Órgãos Dependentes e Tutelados da Casa de Segurança;
   d) Outros responsáveis adstritos à Casa de Segurança autorizados pelo Ministro de Estado e Chefe da Casa de Segurança.

4. O Conselho Técnico da Casa de Segurança reúne-se ordinariamente uma vez por trimestre e extraordinariamente sempre que for convocado pelo Ministro de Estado e Chefe da Casa de Segurança;

b) Acompanhar a situação do asseguramento da assistência sanitária e médico-hospitalar nas Forças Armadas Angolanas e na Polícia Nacional.

3. Os Serviços de Saúde da Casa de Segurança são chefiados por um Chefe de Serviço, que é um oficial general das Forças Armadas Angolanas, nomeado em comissão de serviço pelo Presidente da República, sob proposta do Ministro de Estado e Chefe da Casa de Segurança.

4. Os Serviços de Saúde da Casa de Segurança regem-se por regulamento interno aprovado pelo Ministro de Estado e Chefe da Casa de Segurança.

ARTIGO 27.º
(Centro de Direcção, Telecomunicações e Informática)

1. O Centro de Direcção, Telecomunicações e Informática do Presidente da República e Comandante-Em-Chefe é uma unidade especializada destinada a assegurar os meios técnicos de direcção superior do Presidente da República e Comandante-Em-Chefe.

2. Ao Centro de Direcção, Telecomunicações e Informática do Presidente da República e Comandante-Em-Chefe compete o seguinte:

a) Assegurar as telecomunicações e tecnologias de informação de direcção do Presidente da República e Comandante-Em-Chefe;

b) Assegurar o Centro de Dados da Casa de Segurança.

3. O Centro de Direcção, Telecomunicações e Informática do Presidente da República é chefiado por um Chefe de Unidade que é um oficial general das Forças Armadas Angolanas, nomeado em comissão de serviço pelo Presidente da República, sob proposta do Ministro de Estado e Chefe da Casa de Segurança.

4. O Centro de Direcção, Telecomunicações e Informática do Presidente da República e Comandante-Em-Chefe rege-se por regulamento interno aprovado pelo Ministro de Estado e Chefe da Casa de Segurança.

SECÇÃO V
Organismos Dependentes

ARTIGO 28.º
(Unidade de Segurança Presidencial)

1. A Unidade de Segurança Presidencial (USP) é uma unidade especializada destinada a garantir a segurança do Presidente da República.

2. A Unidade de Segurança Presidencial tem as seguintes atribuições:

a) Garantir a segurança pessoal do Presidente da República e a protecção da sua família;

b) Assegurar a Unidade de Escolta Presidencial para a realização da segurança pessoal do Presidente da República;

c) Garantir a atenção e cuidados de saúde do Presidente da República e da sua família, em articulação com as instituições de saúde afins;

d) Supervisionar as actividades de transporte do Presidente da República e da sua família;

e) Cooperar com o Cerimonial do Presidente da República na fiscalização e cumprimento das regras protocolares relativas aos actos públicos do Presidente da República;

f) Garantir a protecção e vigilância do Palácio Presidencial e das demais instalações presidenciais;

g) Zelar pela manutenção da ordem e da disciplina nas imediações do Palácio Presidencial e das demais instalações presidenciais;

h) Garantir a segurança dos Chefes de Estado e de Governo estrangeiros em visita à República de Angola;

i) Estar em prontidão para, na condição de reserva estratégica, executar outras missões e tarefas que lhe forem atribuídas pelo Presidente da República e Comandante-Em-Chefe, no quadro da segurança e defesa do País.

3. A Unidade de Segurança Presidencial é chefiada por um oficial general das Forças Armadas Angolanas, nomeado em comissão de serviço pelo Presidente da República.

4. A Unidade de Segurança Presidencial rege-se por regulamento interno aprovado pelo Presidente da República, sob proposta do Ministro de Estado e Chefe da Casa de Segurança.

ARTIGO 29.º
(Unidade de Guarda Presidencial)

1. A Unidade de Guarda Presidencial (UGP) é uma unidade especializada destinada a garantir a defesa militar do Presidente da República.

2. A Unidade de Guarda Presidencial tem as seguintes atribuições:

a) Garantir a defesa militar do Presidente da República e a protecção da sua família;

b) Garantir a defesa militar e vigilância do Palácio Presidencial e das demais instalações presidenciais;

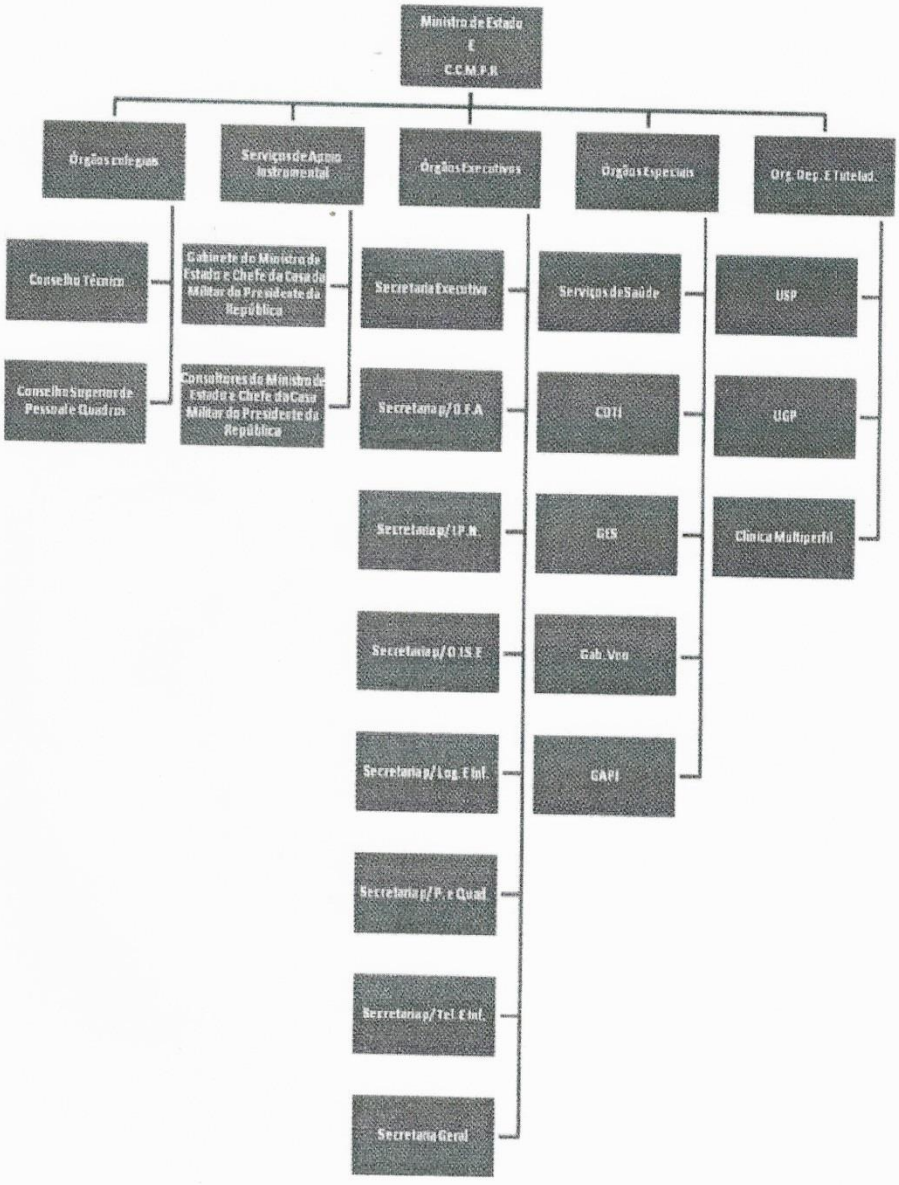
c) Zelar pela manutenção da ordem e da disciplina nas imediações do Palácio Presidencial e das demais instalações presidenciais;

d) Estar em prontidão para, na condição de reserva estratégica, executar outras missões e tarefas que lhe forem acometidas pelo Presidente da República e Comandante-Em-Chefe, no quadro da segurança e defesa do País.

3. A Unidade de Guarda Presidencial é chefiada por um oficial general das Forças Armadas Angolanas nomeado em comissão de serviço pelo Presidente da República.

4. A Unidade de Guarda Presidencial rege-se por regulamento interno aprovado pelo Presidente da República, sob proposta do Ministro de Estado e Chefe da Casa de Segurança.

Organigrama da casa de Segurança do Presidente da República



O Presidente da República, JOSÉ EDUARDO DOS SANTOS.

ANEXO 8

Quarta-feira, 25 de Maio de 2016 I Série – N.º 82

DIÁRIO DA REPÚBLICA

ÓRGÃO OFICIAL DA REPÚBLICA DE ANGOLA

Preço deste número - Kz: 310,00

Toda a correspondência, quer oficial, quer relativa a anúncio e assinaturas do «Diário da República», deve ser dirigida à Imprensa Nacional - E.P., em Luanda, Rua Henrique de Carvalho n.º 2, Cidade Alta, Caixa Postal 1306, www.imprensanacional.gov.ao - End. teleg.: «Imprensa».

ASSINATURA

	Ano
As três séries	Kz: 611 799.50
A 1.ª série	Kz: 361 270.00
A 2.ª série	Kz: 189 150.00
A 3.ª série	Kz: 150 111.00

O preço de cada linha publicada nos Diários da República 1.ª e 2.ª série é de Kz: 75.00 e para a 3.ª série Kz: 95.00, acrescido do respectivo imposto do selo, dependendo a publicação da 3.ª série de depósito prévio a efectuar na tesouraria da Imprensa Nacional - E. P.

SUMÁRIO

PRESIDENTE DA REPÚBLICA

Decreto Presidencial n.º 108/16
de 25 de Maio

Considerando que o Sector das Comunicações Electrónicas está em constante evolução e é fundamental que o quadro legal acompanhe e acomode essa evolução, adaptando-se ao surgimento de novos modelos de negócio, serviços inovadores e produtos que constituam novidade no mercado nacional;

Constatando que o quadro normativo das TIC em Angola, nomeadamente o Regulamento Geral das Comunicações Electrónicas, aprovado em anexo ao Decreto Presidencial n.º 225/11, de 15 de Agosto, teve e tem um papel muito importante na consolidação da liberalização do mercado e na promoção da concorrência, sendo um Diploma inovador e reformador que colocou Angola na rota das melhores práticas a nível internacional;

Reconhecendo que volvidos quase 5 (cinco) anos desde a publicação do pacote normativo das TIC, foram publicados diversos documentos de carácter político e estratégico que reclamam uma reanálise ao quadro normativo em vigor, por forma a verificar se alguns dos mecanismos ali consagrados podem ser actualizados para melhor responder à evolução do sector e alavancar, ainda mais, a contribuição das TIC para o desenvolvimento da economia nacional;

Tendo em conta a aprovação do Plano Estratégico Sobre o Regime de Licenciamento dos Operadores de Comunicações Electrónicas, o qual veio propor um novo enquadramento regulamentar para a oferta de redes e serviços de comunicações electrónicas em Angola, estabelecendo, entre outras coisas, dois novos títulos gerais para o exercício da actividade, as chamadas Licenças Unificadas Globais e as Licenças Multisserviços.

Considerando a necessidade de se proceder a um ajustamento ao actual Regulamento Geral das Comunicações Electrónicas, visando harmonizá-lo com os objectivos estratégicos do Governo;

O Presidente da República decreta, nos termos da alínea l) do artigo 120.º e do n.º 3 do artigo 125.º, ambos da Constituição da República de Angola, o seguinte:

ARTIGO 1.º
(Aprovação)

É aprovado o Regulamento Geral das Comunicações Electrónicas, em anexo ao presente Decreto Presidencial e que dele é parte integrante.

ARTIGO 2.º
(Revogação)

É revogada toda a legislação que contrarie o disposto no presente Diploma, nomeadamente, o Decreto Presidencial n.º 225/11, de 15 de Agosto, que aprova Regulamento Geral das Comunicações Electrónicas e respectivo anexo.

ARTIGO 3.º
(Regime transitório)

Enquanto não forem aprovados os Diplomas de desenvolvimento referidos no Regulamento anexo ao presente Decreto Presidencial, mantêm-se em vigor, na parte em que forem compatíveis com o regime agora afixado, os seguintes actos normativos:

a) Decreto n.º 10/03, de 7 de Março — Aprova o Regulamento do Plano Nacional de Frequências;

b) Decreto n.º 3/04, de 9 de Janeiro — Aprova o Regulamento de Preços dos Serviços Públicos de Telecomunicações de Uso Público;

c) Decreto n.º 13/04, de 12 de Março — Aprova o Regulamento Geral de Interligação de Redes e Serviços de Telecomunicações de Uso Público.

ARTIGO 4.º
(Dúvidas e omissões)

As dúvidas e omissões suscitadas na interpretação e aplicação do presente Diploma são resolvidas pelo Presidente da República.

ARTIGO 5.º
(Entrada em Vigor)

O presente Decreto Presidencial entra em vigor na data da sua publicação.

Apreciado em Conselho de Ministros em [illegible] de Março de 2016.

Publique-se.

Luanda, aos 10 de Maio de 2016.

O Presidente da República José [illegible]

REGULAMENTO GERAL DAS COMUNICAÇÕES ELECTRÓNICAS

TÍTULO I
Disposições Gerais

ARTIGO 1.º
(Objecto)

O presente Regulamento estabelece o regime aplicável às redes e serviços de comunicações electrónicas, às frequências e numeração e ao sector postal.

ARTIGO 2.º
(Âmbito objectivo de aplicação)

1. A oferta de redes e serviços de comunicações electrónicas, assim como a atribuição, [illegible] e numeração ficam sujeitas [illegible] nos respectivos Diplomas de desenvolvimento.

2. Excluem-se do âmbito de aplicação do presente Regulamento:

a) Os serviços que não envolvam controlo editorial sobre os conteúdos transmitidos através de redes de comunicações electrónicas, nomeadamente os serviços [illegible] da sociedade da informação;

b) As redes privadas [illegible] Defesa e Segurança;

c) A rede privativa [illegible]

d) Os serviços [illegible] privativas.

3. O disposto no presente Regulamento não prejudica o regime aplicável à:

a) Utilização do domínio público para efeitos de construção, expansão, instalação ou manutenção de infra-estruturas e redes de comunicações electrónicas;

b) Instalação de infra-estruturas em edifícios e outros espaços;

c) Colocação no mercado de equipamentos terminais de telecomunicações;

d) O regime aplicável ao licenciamento das estações e redes de radiocomunicações;

e) A actividade dos radioamadores.

4. As matérias elencadas no número anterior são especificadas por Diploma da Autoridade das Comunicações Electrónicas ou por Diploma conjunto deste com outras entidades do Executivo, em função da conjugação específica dos domínios a regular.

ARTIGO 3.º
(Âmbito subjectivo de aplicação)

1. Ficam sujeitas ao disposto neste Regulamento e nos respectivos Diplomas de desenvolvimento todas as entidades que oferecem redes ou serviços de comunicações electrónicas, assim como todas as entidades que utilizem frequências ou recursos de numeração para efeitos da exploração de redes ou serviços de comunicações electrónicas.

2. No caso de acordos de interligação transfronteiriços, a entidade que requer o acesso não está sujeita ao presente Regulamento, desde que não ofereça redes ou serviços de comunicações electrónicas em território angolano.

ARTIGO 4.º
(Objectivos de intervenção)

1. Os objectivos específicos de intervenção pública no Sector das Comunicações Electrónicas são os seguintes:

a) Promoção da concorrência na oferta de redes e serviços de comunicações electrónicas;

b) Defesa dos interesses económicos e sociais dos utilizadores;

c) Garantia da existência, disponibilidade e qualidade de redes e serviços de comunicações electrónicas em todo o território nacional, de forma a satisfazer as necessidades de comunicação dos cidadãos e das actividades económicas e sociais;

d) Prestação do serviço universal em todo o território nacional e a adequação do seu âmbito à realidade tecnológica, social e económica de Angola em cada momento;

e) Protecção da privacidade e dos dados pessoais dos utilizadores;

f) Promoção do investimento privado;

g) Garantia da disponibilidade e qualidade das ligações internacionais;

h) Promoção da inovação e desenvolvimento;

i) Disponibilidade, na medida do possível, de frequências e de recursos de numeração adequados para a oferta de redes e serviços de comunicações electrónicas de qualidade em todo o território;

j) Promoção do desenvolvimento do sector, assim como a utilização de novos serviços e novas redes;

k) Garantia da utilização transparente, objectiva e não discriminatória do domínio público;

l) Promoção da divulgação de informações claras, especialmente nos tarifários e nas condições de utilização dos serviços de comunicações electrónicas acessíveis ao público.

2. Os objectivos de intervenção identificados no número anterior são prosseguidos pelas autoridades públicas com competência nesses domínios.

ARTIGO 5.º
(Definições)

1. Para efeitos do disposto no presente Regulamento, entende-se por:

a) «*Acesso*», disponibilização de recursos ou serviços de um operador ou prestador de serviços de comunicações electrónicas a outra empresa para efeitos de prestação de serviços ou de exploração de redes de comunicações electrónicas, abrangendo, nomeadamente, o acesso a elementos de rede, a recursos conexos e a infra-estruturas físicas;

b) «*Acordo de interligação*», acordo celebrado entre dois ou mais operadores de comunicações electrónicas cujo objecto é garantir a interoperabilidade das respectivas redes;

c) «*Circuitos*», alugados meios de uma rede de comunicações electrónicas que proporcionam capacidade de transmissão transparente e dedicada entre pontos terminais, sem envolvimento de funções de comutação controladas pelo utilizador;

d) «*Comunicações electrónicas*», conjunto de sinais suportados e transportados através das plataformas de redes de comunicações electrónicas, incluindo os serviços de telecomunicações e de transmissão de radiodifusão;

e) «*Concessão*», atribuição pelo Poder Executivo, a uma entidade pública ou privada, mediante contrato, do direito de instalar, manter e explorar uma rede ou serviço de comunicações electrónicas, por prazo determinado, sujeitando-se a concessionária aos riscos empresariais, remunerando-se pela cobrança de tarifas aos utilizadores ou por outras receitas alternativas e respondendo directamente pelas suas obrigações e pelos prejuízos que causar;

f) «*Interferência prejudicial*», qualquer interferência que comprometa o funcionamento de um serviço de radionavegação ou de outros serviços de segurança ou que, de outra forma, degrade seriamente,

obstrua ou interrompa repetidamente um serviço de radiocomunicações que opere de acordo com as normas internacionais ou nacionais aplicáveis;

g) «*Interoperabilidade*», funcionalidade que permite a manutenção da comunicação e serviços de forma transparente (ou similar) entre os operadores de comunicações electrónicas;

h) «*Número*», série de dígitos que indica um ponto de terminação de uma rede de comunicações electrónicas e que contém a informação necessária para encaminhar a chamada até esse ponto de terminação;

i) «*Número de emergência*», série de dígitos atribuídos com a finalidade de disponibilizar serviços de comunicações electrónicas de emergência, incluindo, bombeiros, informação pública, polícia, saúde e protecção civil;

j) «*Número geográfico*», número do Plano Nacional de Numeração que contém alguns dígitos com significado geográfico e cuja função é encaminhar as chamadas para o local físico do ponto de terminação da rede;

k) «*Número não geográfico*», número do Plano Nacional de Numeração que não seja um número geográfico, incluindo, nomeadamente, os números móveis, de chamada gratuita ou de tarifa de valor acrescentado;

l) «*Numeração IP*», número não geográfico, estabelecido como número especial, constituído normalmente por quatro ou mais números ou dígitos separados por pontos, que servem para a identificação de computadores, impressoras, routers e/ou mais dispositivos que formam parte de uma rede de comunicações electrónicas;

m) «*Oferta de redes de comunicações electrónicas*», estabelecimento, gestão ou exploração de uma rede de comunicações electrónicas, para efeitos da sua disponibilização, a pessoas singulares ou colectivas, no mercado grossista ou retalhista, tendo em vista a prestação de ou o acesso a serviços de comunicações electrónicas;

n) «*Oferta de serviços de comunicações electrónicas*», disponibilização ou prestação de um serviço de comunicações electrónicas, a pessoas singulares ou colectivas, no mercado grossista ou retalhista;

o) «*Recursos conexos*», serviços associados, as infra-estruturas físicas e outros recursos ou elementos associados a uma rede de comunicações electrónicas ou a um serviço de comunicações electrónicas que permitem ou servem de suporte à oferta de serviços através dessa rede ou serviço, ou que têm potencial para fazê-lo, e incluem, nomeadamente, edifícios ou entradas de edifícios, cablagem de edifícios, antenas, torres e outras estruturas de apoio, condutas, tubagens, postos, câmaras de visita e armários;

p) «*Selecção e pré-selecção de operador*», conjunto de dígitos atribuídos a um operador de comunicações electrónicas que permite ao utilizador escolher o operador que encaminha o curso da chamada nacional e internacional;

q) «*Serviços de áudio-texto*», serviços que se suportam no serviço de comunicações electrónicas, nomeadamente no serviço fixo de telefone ou em serviços telefónicos móveis, e que são destes diferenciáveis em razão do seu conteúdo e natureza específicos;

r) «*Serviços conexos*», serviços associados a uma rede de comunicações electrónicas ou a um serviço de comunicações electrónicas que permitem ou servem de suporte à oferta de serviços através dessa rede ou serviço, ou que têm potencial para fazê-lo, e incluem nomeadamente os sistemas de conversão de números ou os sistemas que ofereçam uma funcionalidade equivalente, os sistemas de acesso condicional e os guias electrónicos de programas, assim como serviços de identidade, localização e presença;

s) «*Serviço universal de comunicações electrónicas*», conjunto mínimo de serviços de comunicações electrónicas considerados essenciais para o desenvolvimento económico e social, de qualidade especificada, disponível para todos os utilizadores, independentemente da sua localização geográfica e, em função das condições nacionais, a um preço acessível;

t) «*IPA*», *software* de interface entre aplicações, disponibilizado por operadores de rádio, televisão ou de distribuição ou fornecedores de serviços, e os recursos no equipamento avançado de televisão digital para serviços de rádio e televisão digitais;

u) «*Oferta de rede aberta*», disponibilização, em termos regulados, de um conjunto de serviços e recursos suportados na rede básica, com a finalidade de promover a oferta de redes ou serviços de comunicações electrónicas em todo o território nacional;

v) «*Dispositivo ilícito*», um equipamento ou programa informático concebido ou adaptado com vista a permitir o acesso ou a visualização de um serviço protegido, sob forma inteligível, sem autorização do prestador do serviço;

w) «*Serviço protegido*», qualquer conteúdo audiovisual, prestado mediante remuneração e com base em acesso condicional.

5. A decisão do Órgão Regulador das Comunicações Electrónicas deve ser sempre fundamentada e notificado ao interessado.

6. A falta de decisão do Órgão Regulador das Comunicações Electrónicas no prazo referido no n.º 4 do presente artigo equivale ao indeferimento do pedido.

ARTIGO 32.º
(Suspensão e extinção da licença)

1. Sem prejuízo de outros casos previstos na lei, a licença suspende-se em caso de interdição temporária para o exercício da actividade determinada pelo Órgão Regulador das Comunicações Electrónicas, nos termos previstos neste Regulamento.

2. A licença extingue-se por caducidade ou revogação.

3. A licença caduca:

a) No termo do prazo, não havendo pedido de renovação ou, havendo pedido, no caso de oposição à renovação por parte do Órgão Regulador das Comunicações Electrónicas;

b) Aquando da cessação da actividade, ou interdição definitiva, por parte do respectivo titular;

c) Em caso de impossibilidade objectiva para a oferta de serviços de comunicações electrónicas, nomeadamente a inexistência de frequências ou recursos de numeração necessários para o exercício da actividade.

4. A licença pode ser revogada por decisão fundamentada do Órgão Regulador das Comunicações Electrónicas em caso de:

a) Incumprimento das normas consignadas no presente Regulamento;

b) Incumprimento das condições indicadas no respectivo título habilitante.

5. Em caso de caducidade ou revogação da licença, compete ao Órgão Regulador das Comunicações Electrónicas adoptar as medidas necessárias de forma a garantir a protecção do utilizador e a salvaguarda da concorrência.

SECÇÃO IV
Comunicação

ARTIGO 33.º
(Requisitos gerais)

1. A oferta de redes de comunicações electrónicas privativas ou de serviços de comunicações electrónicas não acessíveis ao público deve ser comunicada ao órgão regulador, no modelo a aprovar por esta entidade, com uma antecedência de 15 (quinze) dias em relação à data de início da respectiva actividade.

2. Após o decurso do prazo referido no número anterior, a entidade notificante pode iniciar imediatamente a actividade.

3. As entidades que ofereçam redes de comunicações electrónicas privativas ou que disponibilizem serviços de comunicações electrónicas não acessíveis ao público têm de cumprir o disposto no presente Regulamento e nos Diplomas de desenvolvimento, nas partes que lhes forem aplicáveis, e ficam sujeitas à fiscalização do Órgão Regulador das Comunicações Electrónicas.

ARTIGO 34.º
(Suspensão e interdição da actividade)

A oferta de redes de comunicações electrónicas privativas ou de serviços de comunicações electrónicas não acessíveis ao público pode ser suspensa ou interdita por decisão fundamentada do órgão regulador de comunicações electrónicas, nomeadamente em caso de incumprimento das regras consignadas neste Regulamento ou nos Diplomas de desenvolvimento.

SECÇÃO V
Registo

ARTIGO 35.º
(Registo de operadores de comunicações electrónicas)

1. Compete ao Órgão Regulador das Comunicações Electrónicas manter, actualizar de forma regular e divulgar, nomeadamente no seu sítio da internet, um registo dos operadores de comunicações electrónicas com actividade em Angola, o qual, no mínimo, deve conter a seguinte informação:

a) Identificação completa do operador;

b) Morada da sede e sítio electrónico do respectivo operador, se aplicável;

c) Título habilitante emitido e respectivo prazo de duração;

d) Serviços prestados;

e) Zona geográfica de actuação;

f) Direitos de utilização individual de frequências e de numeração atribuídos.

2. Compete aos operadores de comunicações electrónicas fornecerem a informação necessária ao Órgão Regulador das Comunicações Electrónicas para efeitos de inscrição ou actualização do registo, tendo este o poder de solicitar aos operadores em causa as informações que considerar relevantes para estes efeitos.

CAPÍTULO III
Condições e Direitos

ARTIGO 36.º
(Condições gerais)

1. Sem prejuízo de outras condições previstas na legislação aplicável, a oferta de redes e serviços de comunicações electrónicas acessíveis ao público fica sujeita às seguintes condições:

a) Respeito das condições e limites definidos na legislação aplicável;

b) Interoperabilidade dos serviços e interligação das redes;

c) Obrigações de acesso;

d) Garantia da integridade das redes públicas de comunicações electrónicas, nomeadamente, mediante condições que impeçam a interferência electromagnética entre redes e serviços de comunicações electrónicas e respectivas medidas regulamentares;

e) Garantia de comunicações durante calamidades, catástrofes, guerras, entre serviços de emergência e as autoridades;

f) Segurança das redes públicas contra o acesso não autorizado, nos termos da legislação aplicável à protecção de dados pessoais e da privacidade no domínio das comunicações electrónicas e de outra legislação aplicável;

g) Requisitos de protecção do ambiente ou de ordenamento urbano e territorial, incluindo requisitos de partilha de locais, recursos ou infra- estruturas;

h) Protecção de dados pessoais e da privacidade no domínio específico das comunicações electrónicas, em conformidade com a legislação aplicável;

i) Regras específicas de protecção dos utilizadores no Sector das Comunicações Electrónicas;

j) Medidas relativas à limitação da exposição da população aos campos electromagnéticos criados pelas redes de comunicações electrónicas;

k) Instalação, a expensas próprias, e disponibilização de sistemas de intercepção legal de comunicações às autoridades nacionais competentes, bem como fornecimento dos meios de desencriptação ou decifração sempre que ofereçam essas facilidades;

l) Obrigações de transporte nos termos previstos neste Regulamento;

m) Restrições respeitantes à transmissão de conteúdos ilegais, em conformidade com a legislação aplicável;

n) Contribuições financeiras para o Fundo de Apoio ao Desenvolvimento das Comunicações;

o) Pagamento de taxas;

p) Informações a fornecer nos termos previstos neste Regulamento;

q) Abster-se de práticas restritivas da concorrência no âmbito da oferta de redes ou serviços de comunicações electrónicas.

2. Compete ao Órgão Regulador das Comunicações Electrónicas especificar, de entre as referidas no número anterior, as condições aplicáveis consoante o tipo de título habilitante aplicável, devendo fazê-lo de uma forma adequada, não discriminatória, objectiva, transparente e proporcionada.

3. Para efeitos do disposto no número anterior, o Órgão Regulador das Comunicações Electrónicas pode categorizar as condições aplicáveis consoante o tipo de título aplicável, bem como determinar quais as condições aplicáveis à oferta de redes privativas ou serviços de comunicações electrónicas não acessíveis ao público, devendo publicitar tal decisão.

ARTIGO 37.º
(Condições específicas)

A definição de condições gerais, ao abrigo do artigo anterior, não prejudica a imposição, a determinadas entidades, de condições ou obrigações específicas, nos termos previstos neste Regulamento, nomeadamente no Título III.

ARTIGO 38.º
(Direitos gerais dos operadores)

1. Constituem direitos dos operadores de comunicações electrónicas acessíveis ao público, os seguintes:

a) Negociar a interligação e obter o acesso ou a interligação de entidades que oferecem redes ou serviços de comunicações electrónicas acessíveis ao público;

b) Aceder à rede básica;

c) Requerer a expropriação e a constituição de servidões indispensáveis à instalação, protecção e conservação dos respectivos sistemas, equipamentos e demais recursos;

d) Utilizar o domínio público, em condições de igualdade, para efeitos de instalação, passagem ou atravessamento de sistemas, equipamentos e outros recursos;

e) Utilizar o espectro radioeléctrico e os recursos de numeração;

f) Ser remunerado pelos serviços, grossistas e retalhistas, que prestar.

2. Constituem direitos dos operadores de comunicações não acessíveis ao público:

a) Negociar a interligação e o acesso com outros operadores; e

b) Requerer a utilização do domínio público, nos termos gerais.

ARTIGO 39.º
(Direitos de utilização de bens do domínio público)

1. A atribuição de direitos de utilização sobre bens do domínio público, no âmbito das comunicações electrónicas, obedece ao disposto no presente Regulamento e em legislação específica.

2. Os procedimentos para a utilização de bens do domínio público nas comunicações electrónicas devem ser transparentes, publicitados, céleres e não discriminatórios, devendo as condições aplicáveis ao exercício desses direitos obedecer aos princípios da transparência e da não discriminação.

3. Todas a entidades com jurisdição sobre bens do domínio público devem aplicar procedimentos transparentes, céleres e não discriminatórios no que respeita ao exercício do direito de utilização de bens do domínio público, devendo tais condições ser comunicadas ao Órgão Regulador das Comunicações Electrónicas.

CAPÍTULO IV
Exploração

SECÇÃO I
Regras Gerais

ARTIGO 40.º
(Normas executivas)

Compete à Autoridade das Comunicações Electrónicas aprovar os Diplomas necessários para dar cumprimento ao disposto no presente capítulo.

ARTIGO 41.º
(Integridade da rede e disponibilidade dc serviços)

1. Os operadores de comunicações electrónicas acessíveis ao público estão obrigados a assegurar a integridade das respectivas redes e a assegurar a disponibilidade das mesmas em situações de emergência e de força maior.

2. Para efeitos do disposto no número anterior, as entidades ali referidas devem adoptar medidas técnicas e organizacionais apropriadas para gerir de forma adequada os riscos para a segurança das redes e serviços, em particular no que diz respeito à minimização do impacto dos incidentes de segurança nos utilizadores e nas redes interligadas, devendo assegurar, tendo em conta o estado da técnica, um nível de segurança permanentemente adequado.

3. Os operadores de comunicações electrónicas acessíveis ao público devem notificar o Órgão Regulador das Comunicações Electrónicas em caso de violação da segurança ou perda da integridade que tenha um impacto significativo no funcionamento da rede ou serviços.

4. Os operadores de comunicações electrónicas acessíveis ao público devem garantir o acesso ininterrupto aos serviços de emergência.

ARTIGO 42.º
(Obrigações de informação)

1. Os operadores de comunicações electrónicas acessíveis ao público ficam obrigados a publicar e a disponibilizar informações claras, completas, actualizadas sobre os níveis de qualidade de serviço que praticam, preços aplicáveis e termos e condições contratuais habituais.

2. Para efeitos do disposto no número anterior, devem aquelas entidades, no mínimo, publicar e disponibilizar, na forma a definir pelo Órgão Regulador das Comunicações Electrónicas, as seguintes informações:

a) Identificação social;
b) Descrição detalhada dos serviços oferecidos;
c) Preços aplicáveis, abrangendo impostos aplicáveis, todos os tipos de encargos, bem como informações detalhadas sobre os descontos disponíveis;
d) Sistemas de indemnização ou reembolso;
e) Tipos e serviços de manutenção oferecidos;
f) Informações técnicas e de tráfego;
g) Condições contratuais típicas, incluindo períodos mínimos de fidelização, se existentes; e
h) Mecanismos de resolução de litígios, incluindo os criados pela empresa que oferece o serviço.

3. As entidades referidas no n.º 1 do presente artigo devem disponibilizar regularmente à Autoridade das Comunicações Electrónicas e ao Órgão Regulador das Comunicações Electrónicas informações actualizadas incluindo os elementos referidos no presente artigo, sendo o formato, conteúdo e periodicidade definidos pelo Órgão Regulador das Comunicações Electrónicas.

ARTIGO 43.º
(Obrigatoriedade e prioridades de transmissão)

1. Constitui obrigação de todos os operadores de comunicações electrónicas acessíveis ao público a transmissão, com prioridade absoluta, de mensagens motivadas por circunstâncias de força maior, nomeadamente, em caso de catástrofes, calamidades, epidemias ou alteração da ordem pública.

2. Os operadores de redes de comunicações electrónicas privativas ficam igualmente obrigados a transmitir por essa rede, com prioridade absoluta, toda e qualquer mensagem nas condições do número anterior.

3. As comunicações electrónicas do Estado gozam de prioridade sobre as outras comunicações, desde que o pedido seja fundamentado e fique salvaguardado o estabelecido no n.º 1 do presente artigo.

ARTIGO 44.º
(Obrigações de transporte)

1. As entidades que oferecem redes de comunicações electrónicas utilizadas para a distribuição de emissões de serviços de radiodifusão e televisão ao público podem ficar obrigadas, por decisão da Autoridade das Comunicações Electrónicas, a transportar determinados canais e serviços de rádio ou de televisão, nomeadamente os canais e serviços de radiodifusão e televisão de serviço público.

2. As obrigações previstas no número anterior apenas podem ser impostas quando tal seja necessário para a realização de objectivos de interesse geral claramente definidos e devem ser razoáveis, proporcionais, transparentes e sujeitas a uma revisão periódica.

3. O Órgão Regulador das Comunicações Electrónicas pode determinar uma remuneração adequada como contrapartida pelas obrigações de transporte impostas, a qual deve ser aplicada de modo proporcional e transparente.

4. O Órgão Regulador das Comunicações Electrónicas deve ainda estabelecer mecanismos de coordenação com as entidades públicas com jurisdição sobre conteúdos televisivos ou radiofónicos.

SECÇÃO II
Protecção dos Utilizadores e Assinantes

ARTIGO 45.º
(Direitos gerais dos utilizadores e assinantes)

Constituem direitos dos utilizadores de serviços de comunicações electrónicas acessíveis ao público:

a) Utilizar as redes e serviços de comunicações electrónicas acessíveis ao público em condições de igualdade, transparência e não discriminação com os níveis de qualidade obrigatórios;
b) Dispor, em tempo útil e previamente à celebração de qualquer contrato, de informação clara e acessível sobre as condições de acesso e utilização da rede ou serviço;
c) Obter facturação detalhada, quando assim o solicitem;
d) Obter acesso a serviços áudio-texto originariamente barrados;

3. É da responsabilidade do Órgão Regulador das Comunicações Electrónicas determinar as regras necessárias à execução do processo de portabilidade de números.

SECÇÃO III
Acesso e Interligação

ARTIGO 53.º
(Regras gerais)

1. A interligação entre redes públicas de comunicações electrónicas é obrigatória.

2. Compete à Autoridade das Comunicações Electrónicas a criação de um ponto de convergência nacional de comunicações e serviços onde todos os operadores de comunicações electrónicas acessíveis ao público devem estar obrigatoriamente conectados.

3. A interligação entre as várias redes públicas de comunicações electrónicas deve resultar numa rede nacional de comunicações electrónicas plenamente integrada e com acessibilidade universal, para benefício dos seus utilizadores e do público em geral.

4. O acesso aos recursos e serviços de qualquer rede pública de comunicações electrónicas deve ser concedido numa base não discriminatória e equitativa.

5. Sem prejuízo das competências do Órgão Regulador das Comunicações Electrónicas e das suas deliberações, os operadores de comunicações electrónicas são livres de negociar e acordar entre si modalidades técnicas e comerciais de acesso e interligação.

6. Os serviços de acesso e interligação devem ser prestados em termos não discriminatórios e transparentes.

7. Os preços dos serviços de interligação não podem constituir uma barreira à livre comunicação entre utilizadores de diferentes operadores de comunicações electrónicas acessíveis ao público.

8. Toda e qualquer recusa de um pedido de interligação deve ser expressamente fundamentada.

9. Na falta de acordo, qualquer operador pode remeter o caso para o Órgão Regulador das Comunicações Electrónicas, para que seja tomada uma decisão vinculativa nos termos do artigo seguinte.

10. Os acordos de interligação celebrados devem ser enviados ao Órgão Regulador das Comunicações Electrónicas, garantindo este a confidencialidade dos mesmos.

ARTIGO 54.º
(Competências do Órgão Regulador das Comunicações Electrónicas)

1. De forma a garantir o acesso e a interligação nos termos previstos neste Regulamento, compete ao Órgão Regulador das Comunicações Electrónicas:

a) Incentivar o acesso e a interligação, assim como a interoperabilidade de serviços, tendo em vista promover a eficiência e a concorrência sustentável e proporcionar o máximo de benefício aos utilizadores;

b) Determinar as obrigações em matéria de acesso e interligação aos operadores de comunicações electrónicas, incluindo no que se refere os acordos já celebrados;

c) Assegurar a disponibilidade de interligação em todos os pontos em que tal seja tecnicamente viável;

d) Intervir, a pedido ou por iniciativa própria, em caso de falta de acordo entre os operadores, a fim de garantir o cumprimento dos objectivos referidos no artigo 4.º do presente Regulamento.

2. Os operadores de comunicações electrónicas visados devem cumprir as determinações do Órgão Regulador das Comunicações Electrónicas, na forma, modo e prazo estabelecidos.

3. Compete à Autoridade das Comunicações Electrónicas responsável detalhar, em Diploma próprio, os requisitos técnicos, procedimentais e as modalidades de interligação entre as diferentes redes, incluindo regras sobre IP.

ARTIGO 55.º
(Propriedade do tráfego)

Salvo acordo em contrário, a propriedade do tráfego pertence à entidade que explora a rede ou presta o serviço de comunicações electrónicas onde o tráfego é originado, podendo o respectivo encaminhamento, bem como o ponto de entrega, ser livremente negociado entre as partes.

ARTIGO 56.º
(Confidencialidade)

1.Os operadores de comunicações electrónicas devem respeitar a confidencialidade das informações recebidas, transmitidas ou armazenadas na negociação e durante a execução de acordos de acesso ou interligação e utilizá-las exclusivamente para os fins a que se destinam.

2. As informações recebidas não devem ser transmitidas a outras partes, incluindo outros departamentos, filiais ou empresas associadas, relativamente às quais o conhecimento destas possa constituir uma vantagem competitiva.

3. O disposto nos números anteriores não prejudica o exercício dos poderes de supervisão e fiscalização do Órgão Regulador das Comunicações Electrónicas.

SECÇÃO IV
Partilha de Locais e Recursos

ARTIGO 57.º
(Acordos de partilha)

Os operadores de comunicações electrónicas devem promover entre si a celebração de acordos com vista à partilha de locais, recursos instalados ou a instalar, e infra-estruturas.

ARTIGO 58.º
(Obrigatoriedade de partilha)

1. O Órgão Regulador das Comunicações Electrónicas pode determinar a partilha de locais, recursos ou infra-estruturas indicadas no número anterior sempre que, por razões relacionadas com a protecção do ambiente, a saúde ou a segurança pública, o património cultural, o ordenamento do território e

4. Sem prejuízo da prerrogativa do Órgão Regulador das Comunicações Electrónicas estabelecida no n.º 4 do artigo anterior, na falta de decisão no prazo referido no número anterior, considera-se o projecto de oferta de referência, ou as suas alterações, aprovado.

ARTIGO 74.º
(Oferta de rede aberta e natureza da rede básica)

Os serviços da oferta de rede aberta devem respeitar a natureza da rede básica, competindo ao Órgão Regulador das Comunicações Electrónicas e à concessionária garantir que a utilização da referida rede e dos seus componentes, por parte dos beneficiários, não altere nem modifique a sua natureza.

SECÇÃO II
Serviços da Oferta de Rede Aberta

SUBSECÇÃO I
Interligação e Acesso

ARTIGO 75.º
(Obrigações de interligação)

1. A concessionária da rede básica fica obrigada a prestar serviços de interligação aos restantes operadores.

2. O Órgão Regulador das Comunicações Electrónicas deve assegurar a disponibilidade de interligação em todos os pontos da rede básica em que seja tecnicamente viável.

3. Constituem obrigações específicas da concessionária da rede básica:

a) Respeitar os princípios da transparência e orientação para os custos na fixação dos preços de interligação;

b) Fixar e publicitar, de forma detalhada, os vários componentes dos preços de interligação cobrados;

c) Publicar uma oferta de referência, nos termos exigidos no presente Regulamento;

d) Dispor de contabilidade separada para a actividade de interligação, por um lado, e para as outras actividades, por outro, devendo a primeira incluir os serviços de interligação prestados à própria entidade e os serviços prestados a outras entidades;

e) Dispor de um sistema de contabilidade analítica para a actividade de interligação; e

f) Dispor de interface para conexão com os órgãos judiciais, de segurança e ordem pública.

4. Para efeitos do disposto na alínea a) do número anterior, compete à entidade que oferece a interligação demonstrar que os preços de interligação são calculados a partir dos custos reais do serviço, incluindo uma taxa razoável de remuneração do capital investido, tendo em conta os riscos assumidos.

5. O Órgão Regulador das Comunicações Electrónicas pode solicitar à entidade que oferece a interligação que justifique os preços de interligação praticados e, quando adequado, pode determinar o seu ajustamento aos custos, com base na informação da contabilidade analítica.

6. Para efeitos do disposto na alínea d) do n.º 1, a contabilidade da interligação deve identificar todos os custos e proveitos relativos a esta actividade, incluindo uma discriminação dos custos de estrutura e os associados aos activos fixos, bem como identificar pormenorizadamente as bases dos cálculos efectuados e os métodos de afectação utilizados na obtenção daquela informação.

ARTIGO 76.º
(Outras obrigações de acesso)

De forma a garantir o cumprimento dos objectivos mencionados no artigo 4.º do presente Regulamento e as finalidades da rede básica, o Órgão Regulador das Comunicações Electrónicas pode, desde que o faça de forma fundamentada, objectiva e razoável, impor outras obrigações de acesso e interligação para além das previstas nesta secção, nomeadamente obrigações de partilha de recursos e serviços conexos.

SUBSECÇÃO II
Circuitos Alugados

ARTIGO 77.º
(Oferta de circuitos alugados)

1. A empresa concessionária da rede básica fica obrigada a disponibilizar uma oferta de circuitos alugados.

2. Compete ao Órgão Regulador das Comunicações Electrónicas definir as condições da oferta de circuitos alugados nos termos exigidos neste Regulamento.

3. Os preços a cobrar pelo fornecimento de circuitos, bem como os descontos a realizar, devem obedecer aos princípios fundamentais de orientação para os custos, da transparência e da não discriminação.

4. Deve ser implementado um sistema de contabilidade analítica adequado à aplicação do sistema de preços previsto no artigo anterior, sendo da responsabilidade do Órgão Regulador das Comunicações Electrónicas a sua aprovação.

CAPÍTULO IV
Operadores com Poder de Mercado Significativo

ARTIGO 78.º
(Requisitos gerais)

1. Compete ao Órgão Regulador das Comunicações Electrónicas determinar, declarar e publicar, anualmente, a lista dos operadores que dispõem de poder de mercado significativo, com base numa avaliação, de direito e de facto, realizada segundo os seguintes critérios:

a) Capacidade de influenciar as condições de mercado;

b) Quotas de mercado;

c) Relação entre o volume de vendas e a dimensão de mercado;

d) Controlo de meios de acesso aos utilizadores finais;

e) Facilidade de acesso a recursos financeiros.

2. Podem ser declaradas com poder de mercado significativo duas ou mais empresas que actuam concertadamente num mercado (ou região) ou um conjunto de empresas que, embora juridicamente distintas, mantêm entre si laços de interdependência ou subordinação.

3. Sem prejuízo do disposto no n.º 1 do presente artigo, caso se verifiquem alterações significativas nas condições de direito e de facto que estiveram na base da definição dos operadores